

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-189015

(43)Date of publication of application : 10.07.2001

(51)Int.Cl. G11B 7/004
G11B 7/24
G11B 19/04
G11B 19/12
G11B 20/10
G11B 20/12
H04L 9/08

(21)Application number : 2000-125933

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 26.04.2000

(72)Inventor : NAGAI TAKAHIRO
ISHIHARA SHUJI
TAKAGI YUJI
YUMIBA TAKASHI
SHOJI MAMORU
OSHIMA MITSUAKI
OHARA SHUNJI
ITOU MOTOYUKI
ISHIDA TAKASHI
NAKAMURA ATSUSHI
SHIYABANA MASAJI
NAKADA KOHEI

(30)Priority

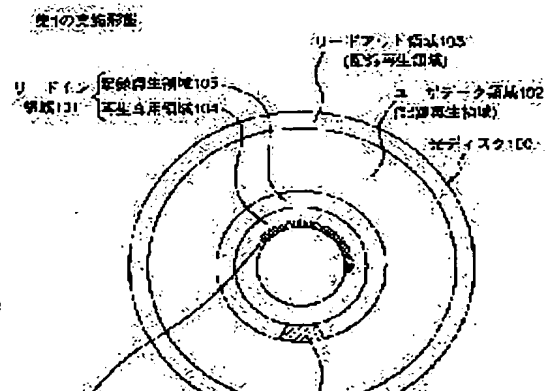
Priority number : 11122104	Priority date : 28.04.1999	Priority country : JP
11128197	10.05.1999	JP
11299635	21.10.1999	JP

(54) OPTICAL DISK, OPTICAL DISK RECORDER, OPTICAL DISK REPRODUCER, OPTICAL DISK RECORDING/REPRODUCING DEVICE, OPTICAL DISK RECORDING/REPRODUCING METHOD, OPTICAL DISK RECORDING METHOD, OPTICAL DISK REPRODUCING METHOD, OPTICAL DISK DELETING METHOD, AND INFORMATION PROCESSING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the unauthorized digital copy from a recording type optical disk to other recording type optical disks.

SOLUTION: In the recording type optical disk capable of recording data, the data recording/reproducing area for recording and reproducing the data and the disk discriminating information area for reproduction only to record the disk discriminating information for discriminating the optical disk are included. This discriminating information is formed by removing the reflection film on the optical disk to the stripe state. The above disk discriminating information includes disk discriminators intrinsic for each optical disk. Also, the



data recording/reproducing area includes the area for recording the data ciphered by using the information including the disk discriminating information for discriminating the optical disk as a key.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-189015

(P2001-189015A)

(43)公開日 平成13年7月10日 (2001.7.10)

(51)Int. Cl. ¹	識別記号	F I	テーマコード(参考)
G 1 1 B 7/004		G 1 1 B 7/004	C 5 D 0 2 9
7/24	5 2 2	7/24	5 2 2 Z 5 D 0 4 4
	5 3 8		5 3 8 P 5 D 0 6 6
			5 3 8 G 5 D 0 9 0
	5 7 1		5 7 1 A 5 J 1 0 4

審査請求 未請求 請求項の数73 O L (全 57 頁) 最終頁に続く

(21)出願番号	特願2000-125833(P2000-125833)	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成12年4月28日 (2000.4.28)	(72)発明者	永井 隆弘 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(31)優先権主張番号	特願平11-122104	(72)発明者	石原 秀志 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(32)優先日	平成11年4月28日 (1999.4.28)	(74)代理人	100062144 弁理士 青山 稔 (外2名)
(33)優先権主張国	日本 (J P)		
(31)優先権主張番号	特願平11-128197		
(32)優先日	平成11年5月10日 (1999.5.10)		
(33)優先権主張国	日本 (J P)		
(31)優先権主張番号	特願平11-299635		
(32)優先日	平成11年10月21日 (1999.10.21)		
(33)優先権主張国	日本 (J P)		

最終頁に続く

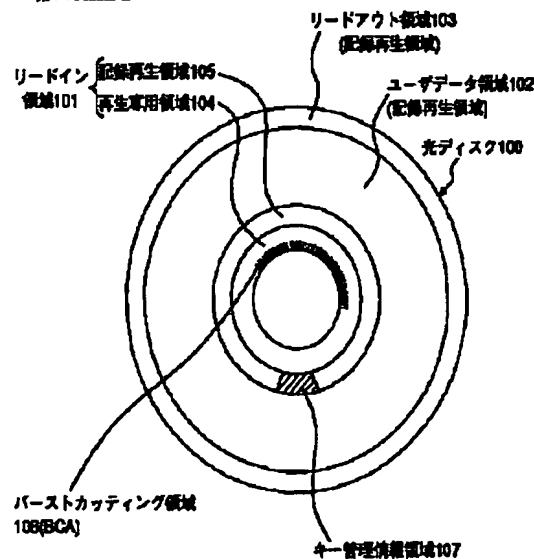
(54)【発明の名称】 光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理シ

(57)【要約】

【課題】 記録型光ディスクから他の記録型光ディスクへの不正なデジタルコピーを防止する。

【解決手段】 データを記録することができる記録型光ディスクにおいて、データを記録して再生するデータ記録再生領域と、上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域とを含む。上記ディスク識別情報は、上記光ディスク上の反射膜をストライプ状に除去することにより形成される。上記ディスク識別情報は、各光ディスク毎に固有なディスク識別子を含む。また、上記データ記録再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータを記録する領域を含む。

第1の実施形態



【特許請求の範囲】

【請求項1】 データを記録することができる記録型光ディスクにおいて、

データを記録して再生するデータ記録再生領域と、

上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域とを含むことを特徴とする光ディスク。

【請求項2】 上記ディスク識別情報は、上記光ディスク上の反射膜をストライプ状に除去することにより形成されたことを特徴とする請求項1記載の光ディスク。

【請求項3】 上記ディスク識別情報は、各光ディスク毎に固有なディスク識別子を含むことを特徴とする請求項1記載の光ディスク。

【請求項4】 上記データ記録再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータを記録する領域を含むことを特徴とする請求項1記載の光ディスク。

【請求項5】 上記暗号化されたデータは、画像データと音楽データとのうちの少なくとも一方であるコンテンツのデータを含むことを特徴とする請求項4記載の光ディスク。

【請求項6】 上記暗号化されたデータは、コンテンツのデータに施された暗号を解くためのデスクランブルキーを含むことを特徴とする請求項4又は5記載の光ディスク。

【請求項7】 上記暗号化されたデータは、コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含むことを特徴とする請求項4又は5記載の光ディスク。

【請求項8】 データを記録することができる記録型光ディスクにおいて、
上記光ディスクは、データを記録して再生するデータ記録再生領域を含み、

上記データ記録再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを記録する領域を含むことを特徴とする光ディスク。

【請求項9】 上記コンテンツのデータと、上記デスクランブルキーは、同一のセクタ内に記録されたことを特徴とする請求項8記載の光ディスク。

【請求項10】 上記コンテンツのデータと、上記デスクランブルキーは異なるセクタに記録されたことを特徴とする請求項8記載の光ディスク。

【請求項11】 上記コンテンツが記録されたセクタに、上記デスクランブルキーが記録される領域を示すポインタを記録したことを特徴とする請求項10記載の光ディスク。

【請求項12】 データを記録することができる記録型

光ディスクにおいて、

上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域と、

暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータを記録して再生するデータ記録再生領域と、

上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとを記録するキー管理情報領域とを含むことを特徴とする光ディスク。

【請求項13】 データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生装置であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域から上記ディスク識別情報を再生する再生手段と、

上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御する制御手段とを備えたことを特徴とする光ディスク記録再生装置。

【請求項14】 データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、

上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録する記録手段とを備えたことを特徴とする光ディスク記録装置。

【請求項15】 上記暗号化されたデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含むことを特徴とする請求項14記載の光ディスク記録装置。

【請求項16】 上記暗号化されたデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含むことを特徴とする請求項14記載の光ディスク記録装置。

【請求項17】 データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化する復号化手段とを備えたことを特徴とする光ディスク再生装置。

【請求項 18】 上記復号化されるデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含むことを特徴とする請求項 17 記載の光ディスク再生装置。

【請求項 19】 上記復号化されるデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含み、

上記復号化手段は、上記デスクランブルキーに含まれる誤りを、上記誤り検出コードに基づいて検出することを特徴とする請求項 17 記載の光ディスク再生装置。

【請求項 20】 データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、

暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録する記録手段を備えたことを特徴とする光ディスク記録装置。

【請求項 21】 上記記録手段は、上記暗号化されたコンテンツのデータを所定の第 1 のセクタに記録し、上記デスクランブルキーを上記第 1 のセクタとは異なる第 2 のセクタに記録することを特徴とする請求項 20 記載の光ディスク記録装置。

【請求項 22】 上記記録手段は、上記暗号化されたコンテンツのデータが記録された第 1 のセクタに、上記デスクランブルキーが記録された第 2 のセクタ内の領域を示すポインタを記録することを特徴とする請求項 21 記載の光ディスク記録装置。

【請求項 23】 データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、

暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生する再生手段を備えたことを特徴とする光ディスク再生装置。

【請求項 24】 上記再生手段は、上記暗号化されたコンテンツを上記光ディスクの第 1 のセクタから再生し、上記デスクランブルキーを上記第 1 のセクタとは異なる第 2 のセクタから再生することを特徴とする請求項 23 記載の光ディスク再生装置。

【請求項 25】 上記再生手段は、上記暗号化されたコンテンツのデータが記録された第 1 のセクタから、上記

デスクランブルキーが再生される第 2 のセクタ内の領域を示すポインタを再生することを特徴とする請求項 24 記載の光ディスク再生装置。

【請求項 26】 データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録装置であって、記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得する取得手段と、

上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てる割り当て手段とを備えたことを特徴とする光ディスク記録装置。

【請求項 27】 データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録装置であって、

コンテンツのデータを再生するために必要なデスクランブルキーを取得する取得手段と、

上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録する記録手段とを備えたことを特徴とする光ディスク記録装置。

【請求項 28】 データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、

上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるかを判断する判断手段と、

上記コンテンツのデータを上記光ディスクに記録できると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てる割り当て手段と、

記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録する記録手段とを備えたことを特徴とする光ディスク記録装置。

【請求項 29】 データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生装置であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記キー管理情報領域のデータを再生する第1の再生手段と、

上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断する判断手段と、

上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生する第2の再生手段と、

上記ディスク識別情報領域からディスク識別情報を再生する第3の再生手段と、

上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生する復号化手段とを備えたことを特徴とする光ディスク再生装置。

【請求項30】 上記復号化されたデスクランブルキーに、誤り検出コードが付与され、上記復号化手段は、上記復号化されたデスクランブルキーに付与された誤り検出コードに基づいて、上記復号化されたデスクランブルキーにおける誤りの有無を判断し、上記判断結果に基づいて、上記復号化されたデスクランブルキーを再生するか否かを判断することを特徴とする請求項29記載の光ディスク再生装置。

【請求項31】 データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生方法であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域から上記ディスク識別情報を再生するステップと、

上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御するステップとを含むことを特徴とする光ディスク記録再生方法。

【請求項32】 データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生するステップと、

上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項33】 データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生するステップと、

少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化するステップとを含むことを特徴とする光ディスク再生方法。

【請求項34】 データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、

暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録するステップを含むことを特徴とする光ディスク記録方法。

【請求項35】 データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、

暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生するステップを含むことを特徴とする光ディスク再生方法。

【請求項36】 データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録方法であって、記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得するステップと、

上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てるステップとを含むことを特徴とする光ディスク記録方法。

【請求項37】 データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録方法であって、

コンテンツのデータを再生するために必要なデスクランブルキーを取得するステップと、

上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項38】 データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生するステップと、

上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるかを判断するステップと、

上記コンテンツのデータを上記光ディスクに記録することができるかと判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てるステップと、

記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項39】 データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生方法であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記キー管理情報領域のデータを再生するステップと、上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているかを判断するステップと、

上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生するステップと、

上記ディスク識別情報領域からディスク識別情報を再生するステップと、

上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生するステップとを含むことを特徴とする光ディスク再生方法。

【請求項40】 データを記録することができる記録型光ディスクにおいて、

第1のディスク情報を記録する第1の情報領域と、各光ディスクを識別するための第2のディスク情報を記録する第2の情報領域と、

光ビームを当該領域に照射することにより情報データを記録するユーザデータ領域とを含むことを特徴とする光ディスク。

【請求項41】 上記第2のディスク情報は、上記第2の情報領域内の記録膜を、半径方向に長い形状でかつ複数個の領域において部分的に除去することにより記録されたことを特徴とする請求項40記載の光ディスク。

【請求項42】 上記第2の情報領域は、上記第1の情報領域内に配置されたことを特徴とする請求項40又は41記載の光ディスク。

【請求項43】 上記第2の情報領域は、上記第1の情報領域の内周側に配置されたことを特徴とする請求項40又は41記載の光ディスク。

【請求項44】 上記第2の情報領域は、上記第1の情報領域内の一部の領域と、上記第1の情報領域よりも内周側に位置する別の領域とにわたって配置されたことを特徴とする請求項40又は41記載の光ディスク。

【請求項45】 上記第1のディスク情報は、微少な凹凸ビットの形式で記録されたことを特徴とする請求項40乃至44のうちの1つに記載の光ディスク。

【請求項46】 データを記録することができる記録型光ディスクにおいて、

上記光ディスクは、複数のセクタを備えたセクタ構造を有し、

上記各セクタは、セクタヘッダ領域と、暗号化されたデータを記録するメインデータ領域とを含み、

上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも1つの復号鍵を記録する復号鍵情報領域を含み、

上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする光ディスク。

【請求項47】 上記各復号鍵は、所定のサイズを有する複数の分割復号鍵に分割され、

上記複数の分割復号鍵は、連続する複数のセクタの各復号鍵情報領域に記録されたことを特徴とする請求項46記載の光ディスク。

【請求項48】 上記復号鍵の分割数は、エラー訂正に必要な複数のセクタである誤り訂正コード（ECC）ブロックに含まれるセクタ数の約数であることを特徴とする請求項47記載の光ディスク。

【請求項49】 上記各復号鍵は、複数の復号鍵を有する復号鍵テーブルに記録され、

上記暗号化されたデータを復号化するために必要な復号鍵の、上記復号鍵テーブル内の記録位置を示すインデックスは、上記セクタの復号鍵情報領域に記録されたことを特徴とする請求項46記載の光ディスク。

【請求項50】 上記復号鍵テーブルの記録状態を表す

情報として、上記復号鍵テーブルの各復号鍵領域に対する復号鍵状態を記録した復号鍵状態領域が記録された請求項49記載の光ディスク。

【請求項51】 上記復号鍵テーブルは、異なる複数の誤り訂正コード（ECC）ブロックにわたって記録されたことを特徴とする請求項49記載の光ディスク。

【請求項52】 上記各復号鍵は、ファイル管理領域で管理されるファイル単位と、光ディスク上で連続する複数のセクタからなるエクステント単位とのうちの少なくとも一方の単位で管理されて記録されたことを特徴とする請求項499記載の光ディスク。

【請求項53】 データを記録することができる記録型光ディスクにおいて、

上記光ディスクは、データを記録するメインデータ領域を含み、

上記メインデータ領域は、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、

上記非暗号化領域は、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含み、

上記暗号化領域のデータは、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする光ディスク。

【請求項54】 上記メインデータ領域は、データの再生制御のために用いられる制御情報を非暗号化状態で記録する制御情報記録セクタと、データを暗号化状態で記録するデータ記録セクタとを含み、

上記制御情報記録セクタは、上記復号鍵の変換のために用いられる復号鍵変換データを含み、

上記データ記録セクタのデータは上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする請求項53記載の光ディスク。

【請求項55】 上記データ記録セクタは、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、

上記非暗号化領域は別の復号鍵変換データを含み、

上記暗号化領域のAVデータは上記復号鍵変換データを用いて変換された復号鍵をさらに別の第2の復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする請求項54記載の光ディスク。

【請求項56】 上記復号鍵変換データは、少なくともデータのコピー制御情報を含むことを特徴とする請求項53記載の光ディスク。

【請求項57】 データを記録することができる記録型光ディスクにデータを記録するための光ディスク記録方法において、

上記光ディスク上に記録された復号鍵ステータスを読み出し、上記読み出された復号鍵ステータスに基づいて復号鍵の空き領域があるか否かを判断するステップと、
上記復号鍵の空き領域があると判断されたときに、復号

鍵領域を予約して復号鍵を記録するステップと、

ファイル単位とエクステント単位のうちの少なくとも一方の単位で著作権制御情報と復号鍵インデックスを設定するステップと、

上記復号鍵を用いてデータを暗号化して、暗号化されたデータを、ファイル単位とエクステント単位のうちの少なくとも一方の単位で上記光ディスクに記録するステップと、

上記光ディスクに記録されたデータを管理するためのファイル管理情報を上記光ディスクに記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項58】 データを記録することができる記録型光ディスクからデータを再生するための光ディスク再生方法において、

ファイル単位又はエクステント単位で記録された再生すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、

上記取得された復号鍵インデックスに対応する復号鍵を再生して取得するステップと、

上記復号鍵を用いて暗号化されたファイル単位又はエクステント単位のデータを再生するステップとを含むことを特徴とする光ディスク再生方法。

【請求項59】 データを記録することができる記録型光ディスクからデータを削除するための光ディスク削除方法において、

ファイル単位又はエクステント単位で記録された削除すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、

上記取得された復号鍵インデックスに対応し、復号鍵の記録状態を示す復号鍵ステータスを更新して復号鍵を開放するステップと、

上記光ディスクに記録されたデータを管理するためのファイル管理情報から上記削除すべきデータに対応するファイルエントリを削除することにより上記ファイル管理情報を更新するステップとを含むことを特徴とする光ディスク削除方法。

【請求項60】 データを暗号鍵を用いて暗号化するデータ暗号化装置と、

上記データを復号化するために必要な復号鍵を記録型光ディスクに記録して再生する光ディスク記録再生装置と、

上記光ディスク記録再生装置及び上記データ暗号化装置に接続された制御装置とを備えた情報処理システムであって、

上記光ディスク記録再生装置は、

上記光ディスクに復号鍵テーブルを記録し、上記光ディスクから復号鍵テーブルを再生する第1の記録再生手段と、

上記復号鍵を暗号化して上記制御装置に送信し、上記制御装置から暗号化された復号鍵を受信して復号化する暗

号化及び復号化手段と、

上記光ディスクに復号鍵の記録状態を示す復号鍵状態テーブルを記録し、上記光ディスクから復号鍵状態テーブルを再生する第2の記録再生手段とを備え、

上記データ暗号化装置は、

上記復号鍵を暗号化して上記制御装置に送信する暗号化手段を備え、

上記制御装置は、

上記データ暗号化装置の暗号化手段から暗号化された復号鍵を受信する受信手段と、

上記再生された復号鍵状態テーブルに基づいて復号鍵の空き領域を検索し、上記検索された空き領域に、上記受信された暗号化された復号鍵を割り当て、上記割り当てられた暗号化された復号鍵を上記光ディスク記録再生装置に送信する割当手段とを備え、

上記光ディスク記録再生装置の暗号化及び復号化手段は、上記制御装置の割当手段から上記割り当てられた暗号化された復号鍵を受信して復号化することを特徴とする情報処理システム。

【請求項61】 データと、上記データを復号化するために必要な複数の復号鍵を備えた復号鍵テーブルを記録型光ディスクから再生する光ディスク再生装置と、上記光ディスク再生装置に接続された制御装置と、復号鍵を用いてデータを復号化するデータ復号化装置とを備えた情報処理システムであって、

上記光ディスク再生装置は、

上記光ディスクから復号鍵テーブルを再生する第1の再生手段と、

上記再生された復号鍵テーブルを暗号化して、暗号化された復号鍵テーブルを上記制御装置に送信する暗号化手段と、

上記光ディスクから複数の復号鍵の記録状態を示す復号鍵状態テーブルを再生する第2の再生手段とを備え、

上記制御装置は、

上記光ディスク再生装置から上記暗号化された復号鍵テーブルを受信する受信手段と、

上記再生された復号鍵状態テーブルに基づいて、上記受信された復号鍵テーブルから上記光ディスクに記録されたデータを復号化するために必要な暗号化された復号鍵を検索して上記データ復号化手段に送信する検索手段とを備え、

上記データ復号化装置は、

上記暗号化された復号鍵を復号化して復号鍵を生成する第1の復号化手段と、

光ディスク再生装置によって再生された暗号化されたデータを、上記復号化された復号鍵を用いて復号化する第2の復号化手段とを備えたことを特徴とする情報処理システム。

【請求項62】 データを記録することができる記録型光ディスクにデータを記録する光ディスク記録装置にお

いて、

上記光ディスクは、非暗号化領域と、暗号化領域とを含み、

データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録する記録手段を備えたことを特徴とする光ディスク記録装置。

【請求項63】 上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、

上記記録手段は、上記データの再生制御のために用いられる制御情報を上記制御情報記録セクタに非暗号化状態で記録し、上記制御情報に含まれる復号鍵変換データを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録することを特徴とする請求項62記載の光ディスク記録装置。

【請求項64】 上記記録手段は、別の復号鍵変換データを含むデータを非暗号化状態で上記データ記録セクタの非暗号化領域に記録し、上記制御情報に含まれる復号鍵変換データと、上記別の復号鍵変換データとを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録することを特徴とする請求項63記載の光ディスク記録装置。

【請求項65】 データを記録することができる記録型光ディスクからデータを再生する光ディスク再生装置において、

上記光ディスクは、非暗号化領域と、暗号化領域とを含み、

上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生する再生手段を備えたことを特徴とする光ディスク再生装置。

【請求項66】 上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、

上記再生手段は、上記データの再生制御のために用いられる制御情報を制御情報記録セクタから再生し、上記制御情報に含まれる復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生することを特徴とする請求項65記載の光ディスク再生装置。

【請求項67】 上記再生手段は、上記データ記録セクタの非暗号化領域に記録された別の復号鍵変換データを再生し、上記制御情報に含まれる復号鍵変換データと、上記再生された別の復号鍵変換データとを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を

用いて上記データ記録セクタに記録されたデータを復号化して再生することと特徴とする請求項6記載の光ディスク再生装置。

【請求項68】 データを記録することができる記録型光ディスクにデータを記録する光ディスク記録方法において、

上記光ディスクは、非暗号化領域と、暗号化領域とを含み、

データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録するステップを含むことを特徴とする光ディスク記録方法。

【請求項69】 データを記録することができる記録型光ディスクからデータを再生する光ディスク再生方法において、

上記光ディスクは、非暗号化領域と、暗号化領域とを含み、

上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生するステップを含むことを特徴とする光ディスク再生方法。

【請求項70】 記録されたデータを再生するための再生専用型光ディスクにおいて、

データが記録されたデータ再生領域と、

上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域とを含み、

上記データ再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータが記録された領域を含むことを特徴とする光ディスク。

【請求項71】 記録されたデータを再生するための再生専用型光ディスクにおいて、

上記光ディスクは、データが記録されたデータ再生領域を含み、

上記データ再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとが記録された領域を含むことを特徴とする光ディスク。

【請求項72】 記録されたデータを再生するための再生専用型光ディスクにおいて、

上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域と、

暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータが記録されたデータ再生領域と、

上記コンテンツのデータを再生するときに使用するキー

情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとが記録されたキー管理情報領域とを含むことを特徴とする光ディスク。

【請求項73】 記録されたデータを再生するための再生専用型光ディスクにおいて、

上記光ディスクは、複数のセクタを備えたセクタ構造を有し、

上記各セクタは、セクタヘッダ領域と、暗号化されたデータが記録されたメインデータ領域とを含み、

上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも1つの復号鍵が記録された復号鍵情報領域を含み、

上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする光ディスク。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、著作権を有する映画の画像データや音楽の音声データを含むAVデータ(Audio and Visual Data)などのデータが記録されている光ディスクから、他の記録型光ディスクなどの記録媒体への不正なデジタルコピーを防止することができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法、及び情報処理システムに関する。

【0002】

【従来の技術】光ディスクは、従来のテープメディアに比べてランダムアクセス性に優れており、また、レーザ光を利用した非接触な記録及び再生が可能のため繰り返し利用による劣化が少ないという特徴を有している。さらに、光ディスクは、ディスク製造者によるマスタリングによって、安価に大量の複製が可能という特徴を有しており、高音質のデジタルオーディオとしてCD(Compact Disk)が従来のアナログ記録のレコードにとって代わって一般的になっている。さらに、近年、高品質の画像データがデジタル記録されたDVD(Digital Video Disk、又はDigital Versatile Disk)が商品化されAVデータのデジタル記録媒体としての光ディスクが今後さらに発展していくことが予想される。

【0003】一方、音楽CD、CD-ROMやDVD-ROMのように、ディスク製造業者によってデータがブリティットの形式で予め記録されている再生専用の光ディスクだけでなく、近年、ユーザが家庭でAVデータを記録できる、例えば、CD-R、CD-RW、MO、MDやDVD-RAMなどの記録型の光ディスクが開発され、世に広がりつつある。

【0004】また、テレビ放送においても従来のアナログ方式から多チャンネル化や様々なサービスが可能なデジタル方式が導入されており、このような傾向は今後さらに広がっていく。特に、記録型光ディスクは、ディ

デジタル化された放送や通信で配信されてくるコンテンツの記録媒体として、配信時に蓄積した後プログラム選択して視聴するタイムシフト利用を目的の中心としたAVデータの記録に利用されることが予想される。

【0006】従来、コンピュータを中心に利用されてきた記録型の光ディスクは、利用者自らが作成したデータの保存を目的として利用されており、記録型の光ディスク間でのコピーを制限する仕組みを有していなかった。記録型の光ディスクが広く利用されるようになると、記録された光ディスクのデータを、一般ユーザがそのまま他の記録型光ディスクに違法にコピーすることにより、本来そのAVデータの著作権者に支払われるべき著作権料を払うこと無しに、また、デジタル記録が可能ることから自質や画質の劣化なしに不当な複製を入手することが可能になり、良質のコンテンツの広まりを阻害する要因にもなっている。音楽等をデジタル記録するMDでは、記録回数を制限する世代管理を行う仕組みが導入され、世代管理データとともに光ディスクに記録し、その世代管理データによりコピー回数の制限を行っている。

【0006】また、例えば、CD-ROMやDVD-ROMの不正なコピーを防止するために、光ディスクのビット部にバーコードを重ね書きするための追記領域であるバーストカッティング領域(Burst Cutting Area; 以下、BCAという。)を設け、光ディスクの製造時にBCAにディスク毎に異なるIDを記録しておく方法が、国際公開番号WO97/14144号の国際出願において提案されている。この方法によると、パスワードはディスクIDにより異なるので、1つのパスワードは1枚のディスクの暗号しか解読することができなくなり、コンテンツが不正にコピーされてもディスクIDの情報が欠落しているため、コンテンツは解読されなくなる。

【0007】図39は、従来技術のDVD-ROMのユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。DVD-ROMでは、図39に示すように、ディスク上に記録するコンテンツのデータに対して暗号化を行っている。

【0008】図39において、DVD-ROMのユーザデータ領域は、セクタヘッダ領域3201と、メインデータ領域3202と、誤り検出コード3203とから構成される。ここで、セクタヘッダ領域3201には、セクタの位置を示すセクタアドレス3204と、メインデータ領域3202に記録されるデータに関する著作権制御情報(例えば、スクランブルフラグ、コピー制御情報など)が記録される著作権制御情報3205と、メインデータ領域3202のデータに暗号が施されている場合に復号するための復号鍵3206とが記録される。また、メインデータ領域3202には、主に著作権保護を必要とするAVデータなどが暗号化されて記録される。

【0009】このようなユーザデータ領域の再生時には、まず、セクタヘッダ領域3201から暗号化コンテンツの再生に必要な復号鍵3206を得る。取得した復号鍵3206は復号器3207に入力され、復号器3207は入力された復号鍵3206を所定のディスク鍵を用いてコンテンツ復号鍵を復号して、復号器3208に出力する。次いで、復号器3208は、メインデータ領域3202に対応するセクタヘッダ領域3201に格納された著作権制御情報3205に従って、メインデータ領域3202の暗号化コンテンツを上記復号されたコンテンツ復号鍵を用いて復号を行い、再生可能なデータである復号化コンテンツを得る。

【0010】図39に示した構成による光ディスクでは、パーソナルコンピュータのドライブ装置などからメインデータ領域3202に対する読み出しが可能であるが、復号鍵3206を記録した領域を正規の認証機能を有する光ディスク再生装置しか読み出しできないように構成することにより、不正な複製や海賊版の作成を防止できるようにしている。

【0011】

【発明が解決しようとする課題】しかしながら、世代管理データを用いた不正コピー防止方法では、コピー時に世代管理データの変更(“1回コピー可能”から“コピー不可”への情報の変更)が不可欠である。これに対して、光ディスク上のデータを世代管理データとともに変更を加えずコピーしたり、コンピュータ等で世代管理データを改ざんして記録したりすることにより、不正コピーを十分に防止できないという問題点を有していた。さらに、コンテンツとともに予め記録した世代管理データによりコピー回数の制限を行うため、たとえ正規の著作権料を払ったとしても光ディスク上の“コピー不可”となったデータは他の光ディスクへのコピーが全く許されず、利用者はコンテンツ供給者から供給を待たなければならないという問題を有していた。いずれもコンテンツ供給者が利用者の行う記録型光ディスクへのコピーを十分に管理できないことによるものである。

【0012】近年、パーソナルコンピュータが高性能化し、さらにそれらがネットワークに接続されることによって、高性能でかつ、複数台のパーソナルコンピュータによる高速な暗号の解読が行われている。このような解読に対して、より暗号の強度を高めるためには、暗号に使用する鍵の鍵長を拡張することが必要となる。しかしながら、従来から提案されているようなセクタヘッダに復号鍵を記録するような鍵管理方法では、予め決められた長さ(復号鍵領域のサイズ)以下の復号鍵しか記録することができず、将来に暗号の強度を高めるために鍵長を長くできないという問題点があった。

【0013】本発明の第1の目的は、以上の問題点を解決し、コンテンツ供給者が管理できない不正なデジタルコピーを防止できる、光ディスク、光ディスク記録装

置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１４】また、本発明の第２の目的は、以上の問題点を解決し、著作権保護を必要とするデータを復号化するために必要な復号鍵の信頼性をより高めることができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１５】さらに、本発明の第３の目的は、以上の問題点を解決し、記録するコンテンツの著作権保護のレベルに応じて暗号強度の設定することができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１６】

【課題を解決するための手段】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、データを記録して再生するデータ記録再生領域と、上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域とを含むことを特徴とする。

【００１７】上記光ディスクにおいて、上記ディスク識別情報は、好ましくは、上記光ディスク上の反射膜をストライプ状に除去することにより形成される。また、上記光ディスクにおいて、上記ディスク識別情報は、好ましくは、各光ディスク毎に固有なディスク識別子を含む。

【００１８】また、上記光ディスクにおいて、上記データ記録再生領域は、好ましくは、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータを記録する領域を含む。上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、画像データと音楽データとのうちの少なくとも一方であるコンテンツのデータを含む。また、上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。さらに、上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含む。

【００１９】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクは、データを記録して再生するデータ記録再生領域を含み、上記データ記録再生領域は、暗号化された画

像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを記録する領域を含むことを特徴とする。

【００２０】上記光ディスクにおいて、好ましくは、上記コンテンツのデータと、上記デスクランブルキーは、同一のセクタ内に記録され、もしくは、上記コンテンツのデータと、上記デスクランブルキーは異なるセクタに記録される。また、上記光ディスクにおいて、好ましくは、上記コンテンツが記録されたセクタに、上記デスクランブルキーが記録される領域を示すポインタを記録する。

【００２１】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域と、暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータを記録して再生するデータ記録再生領域と、上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとを記録するキー管理情報領域とを含むことを特徴とする。

【００２２】本発明に係る光ディスク記録再生装置は、データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生装置であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域から上記ディスク識別情報を再生する再生手段と、上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御する制御手段とを備えたことを特徴とする。

【００２３】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録する記録手段とを備えたことを特徴とする。

【００２４】上記光ディスク記録装置において、上記暗号化されたデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。また、上記光ディスク記録装置において、上記暗

号化されたデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含む。

【００２５】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化する復号化手段とを備えたことを特徴とする。

【００２６】上記光ディスク再生装置において、上記復号化されるデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。また、光ディスク再生装置において、上記復号化されるデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含み、上記復号化手段は、上記デスクランブルキーに含まれる誤りを、上記誤り検出コードに基づいて検出する。

【００２７】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録する記録手段を備えたことを特徴とする。

【００２８】上記光ディスク記録装置において、上記記録手段は、好ましくは、上記暗号化されたコンテンツのデータを所定の第１のセクタに記録し、上記デスクランブルキーを上記第１のセクタとは異なる第２のセクタに記録する。また、上記光ディスク記録装置において、上記記録手段は、好ましくは、上記暗号化されたコンテンツのデータが記録された第１のセクタに、上記デスクランブルキーが記録された第２のセクタ内の領域を示すポインタを記録する。

【００２９】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生する再生手段を備えたことを特徴とする。

【００３０】上記光ディスク再生装置において、上記再生手段は、好ましくは、上記暗号化されたコンテンツを上記光ディスクの第１のセクタから再生し、上記デスク

ランブルキーを上記第１のセクタとは異なる第２のセクタから再生する。上記光ディスク再生装置において、上記再生手段は、好ましくは、上記暗号化されたコンテンツのデータが記録された第１のセクタから、上記デスクランブルキーが再生される第２のセクタ内の領域を示すポインタを再生する。

【００３１】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録装置であって、記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得する取得手段と、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てる割当手段とを備えたことを特徴とする。

【００３２】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録装置であって、コンテンツのデータを再生するために必要なデスクランブルキーを取得する取得手段と、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録する記録手段とを備えたことを特徴とする。

【００３３】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるか否かを判断する判断手段と、上記コンテンツのデータを上記光ディスクに記録することができるかと判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てる割当手段と、記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録する記録手段とを備えたことを特徴とする。

【００３４】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディス

ク再生装置であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記キー管理情報領域のデータを再生する第1の再生手段と、上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断する判断手段と、上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生する第2の再生手段と、上記ディスク識別情報領域からディスク識別情報を再生する第3の再生手段と、上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生する復号化手段とを備えたことを特徴とする。

【0035】上記光ディスク再生装置において、好ましくは、上記復号化されたデスクランブルキーに、誤り検出コードが付与され、上記復号化手段は、上記復号化されたデスクランブルキーに付与された誤り検出コードに基づいて、上記復号化されたデスクランブルキーにおける誤りの有無を判断し、上記判断結果に基づいて、上記復号化されたデスクランブルキーを再生するか否かを判断する。

【0036】本発明に係る光ディスク記録再生方法は、データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生方法であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域から上記ディスク識別情報を再生するステップと、上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御するステップとを含むことを特徴とする。

【0037】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生するステップと、上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録するステップとを含むことを特徴とする。

【0038】本発明に係る光ディスク再生方法は、デー

タを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生するステップと、少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化するステップとを含むことを特徴とする。

【0039】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録するステップを含むことを特徴とする。

【0040】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生するステップを含むことを特徴とする。

【0041】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録方法であって、記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得するステップと、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てるステップとを含むことを特徴とする。

【0042】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録方法であって、コンテンツのデータを再生するために必要なデスクランブルキーを取得するステップと、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録するステップとを含むことを特徴とする。

【0043】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、上記光ディスクは、上記光ディスクを識別するため

のディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生するステップと、上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるかを判断するステップと、上記コンテンツのデータを上記光ディスクに記録できると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てるステップと、記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録するステップとを含むことを特徴とする。

【0044】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生方法であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記キー管理情報領域のデータを再生するステップと、上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているかを判断するステップと、上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生するステップと、上記ディスク識別情報領域からディスク識別情報を再生するステップと、上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生するステップとを含むことを特徴とする。

【0045】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、第1のディスク情報を記録する第1の情報領域と、各光ディスクを識別するための第2のディスク情報を記録する第2の情報領域と、光ビームを当該領域に照射することにより情報データを記録するユーザデータ領域とを含むことを特徴とする。

【0046】上記光ディスクにおいて、上記第2のディスク情報は、好ましくは、上記第2の情報領域内の記録膜を、半径方向に長い形状でかつ複数個の領域において部分的に除去することにより記録される。また、上記光ディスクにおいて、好ましくは、上記第2の情報領域は、上記第1の情報領域内に配置され、又は、上記第1の情報領域の内周側に配置され、もしくは、上記第2の情報領域は、上記第1の情報領域内の一部の領域と、上記第1の情報領域よりも内周側に位置する別の領域とに

わたって配置される。さらに、上記第1のディスク情報は、好ましくは、微少な凹凸ビットの形式で記録される。

【0047】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクは、複数のセクタを備えたセクタ構造を有し、上記各セクタは、セクタヘッダ領域と、暗号化されたデータを記録するメインデータ領域とを含み、上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも1つの復号鍵を記録する復号鍵情報領域を含み、上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする。

【0048】上記光ディスクにおいて、上記各復号鍵は、好ましくは、所定のサイズを有する複数の分割復号鍵に分割され、上記複数の分割復号鍵は、連続する複数のセクタの各復号鍵情報領域に記録される。ここで、上記復号鍵の分割数は、好ましくは、エラー訂正に必要な複数のセクタである誤り訂正コード(ECC)ブロックに含まれるセクタ数の約数である。また、上記光ディスクにおいて、上記各復号鍵は、好ましくは、複数の復号鍵を有する復号鍵テーブルに記録され、上記暗号化されたデータを復号化するために必要な復号鍵の、上記復号鍵テーブル内の記録位置を示すインデックスは、上記セクタの復号鍵情報領域に記録される。さらに、上記光ディスクにおいて、上記復号鍵テーブルの記録状態を表す情報として、好ましくは、上記復号鍵テーブルの各復号鍵領域に対する復号鍵状態を記録した復号鍵状態領域が記録される。またさらに、上記光ディスクにおいて、上記復号鍵テーブルは、好ましくは、異なる複数の誤り訂正コード(ECC)ブロックにわたって記録される。また、上記光ディスクにおいて、上記各復号鍵は、好ましくは、ファイル管理領域で管理されるファイル単位と、光ディスク上で連続する複数のセクタからなるエクステン単位とのうちの少なくとも一方の単位で管理されて記録される。

【0049】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクは、データを記録するメインデータ領域を含み、上記メインデータ領域は、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、上記非暗号化領域は、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含み、上記暗号化領域のデータは、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする。

【0050】上記光ディスクにおいて、好ましくは、上記メインデータ領域は、データの再生制御のために用いられる制御情報を非暗号化状態で記録する制御情報記録セクタと、データを暗号化状態で記録するデータ記録セクタとを含み、上記制御情報記録セクタは、上記復号鍵

の変換のために用いられる復号鍵変換データを含み、上記データ記録セクタのデータは上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化される。また、上記光ディスクにおいて、好ましくは、上記データ記録セクタは、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、上記非暗号化領域は別の復号鍵変換データを含み、上記暗号化領域のAVデータは上記復号鍵変換データを用いて変換された復号鍵をさらに別の第2の復号鍵変換データを用いて変換された復号鍵を用いて暗号化される。さらに、上記光ディスクにおいて、上記復号鍵変換データは、好ましくは、少なくともデータのコピー制御情報を含む。

【0051】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクにデータを記録するための光ディスク記録方法において、上記光ディスク上に記録された復号鍵ステータスを読み出し、上記読み出された復号鍵ステータスに基づいて復号鍵の空き領域があるか否かを判断するステップと、上記復号鍵の空き領域があると判断されたときに、復号鍵領域を予約して復号鍵を記録するステップと、ファイル単位とエクステン単位うちの少なくとも一方の単位で著作権制御情報と復号鍵インデックスを設定するステップと、上記復号鍵を用いてデータを暗号化して、暗号化されたデータを、ファイル単位とエクステン単位うちの少なくとも一方の単位で上記光ディスクに記録するステップと、上記光ディスクに記録されたデータを管理するためのファイル管理情報を上記光ディスクに記録するステップとを含むことを特徴とする。

【0052】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからデータを再生するための光ディスク再生方法において、ファイル単位又はエクステン単位で記録された再生すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、上記取得された復号鍵インデックスに対応する復号鍵を再生して取得するステップと、上記復号鍵を用いて暗号化されたファイル単位又はエクステン単位のデータを再生するステップとを含むことを特徴とする。

【0053】本発明に係る光ディスク削除方法は、データを記録することができる記録型光ディスクからデータを削除するための光ディスク削除方法において、ファイル単位又はエクステン単位で記録された削除すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、上記取得された復号鍵インデックスに対応し、復号鍵の記録状態を示す復号鍵ステータスを更新して復号鍵を開放するステップと、上記光ディスクに記録されたデータを管理するためのファイル管理情報から上記削除すべきデータに対応するファイルエントリを削除することにより上記ファイル管理情報を更新するス

テップとを含むことを特徴とする。

【0054】本発明に係る情報処理システムは、データを暗号鍵を用いて暗号化するデータ暗号化装置と、上記データを復号化するために必要な復号鍵を記録型光ディスクに記録して再生する光ディスク記録再生装置と、上記光ディスク記録再生装置及び上記データ暗号化装置に接続された制御装置とを備えた情報処理システムであって、上記光ディスク記録再生装置は、上記光ディスクに復号鍵テーブルを記録し、上記光ディスクから復号鍵テーブルを再生する第1の記録再生手段と、上記復号鍵を暗号化して上記制御装置に送信し、上記制御装置から暗号化された復号鍵を受信して復号化する暗号化及び復号化手段と、上記光ディスクに復号鍵の記録状態を示す復号鍵状態テーブルを記録し、上記光ディスクから復号鍵状態テーブルを再生する第2の記録再生手段とを備え、上記データ暗号化装置は、上記復号鍵を暗号化して上記制御装置に送信する暗号化手段を備え、上記制御装置は、上記データ暗号化装置の暗号化手段から暗号化された復号鍵を受信する受信手段と、上記再生された復号鍵状態テーブルに基づいて復号鍵の空き領域を検索し、上記検索された空き領域に、上記受信された暗号化された復号鍵を割り当て、上記割り当てられた暗号化された復号鍵を上記光ディスク記録再生装置に送信する割り当て手段とを備え、上記光ディスク記録再生装置の暗号化及び復号化手段は、上記制御装置の割り当て手段から上記割り当てられた暗号化された復号鍵を受信して復号化することを特徴とする。

【0055】本発明に係る情報処理システムは、データと、上記データを復号化するために必要な複数の復号鍵を備えた復号鍵テーブルを記録型光ディスクから再生する光ディスク再生装置と、上記光ディスク再生装置に接続された制御装置と、復号鍵を用いてデータを復号化するデータ復号化装置とを備えた情報処理システムであって、上記光ディスク再生装置は、上記光ディスクから復号鍵テーブルを再生する第1の再生手段と、上記再生された復号鍵テーブルを暗号化して、暗号化された復号鍵テーブルを上記制御装置に送信する暗号化手段と、上記光ディスクから複数の復号鍵の記録状態を示す復号鍵状態テーブルを再生する第2の再生手段とを備え、上記制御装置は、上記光ディスク再生装置から上記暗号化された復号鍵テーブルを受信する受信手段と、上記再生された復号鍵状態テーブルに基づいて、上記受信された復号鍵テーブルから上記光ディスクに記録されたデータを復号化するために必要な暗号化された復号鍵を検索して上記データ復号化手段に送信する検索手段とを備え、上記データ復号化装置は、上記暗号化された復号鍵を復号化して復号鍵を生成する第1の復号化手段と、光ディスク再生装置によって再生された暗号化されたデータを、上記復号化された復号鍵を用いて復号化する第2の復号化手段とを備えたことを特徴とする。

【００５６】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクにデータを記録する光ディスク記録装置において、上記光ディスクは、非暗号化領域と、暗号化領域とを含み、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録する記録手段を備えたことを特徴とする。

【００５７】上記光ディスク記録装置において、好ましくは、上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、上記記録手段は、上記データの再生制御のために用いられる制御情報を上記制御情報記録セクタに非暗号化状態で記録し、上記制御情報に含まれる復号鍵変換データを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録する。また、上記光ディスク記録装置において、上記記録手段は、好ましくは、別の復号鍵変換データを含むデータを非暗号化状態で上記データ記録セクタの非暗号化領域に記録し、上記制御情報に含まれる復号鍵変換データと、上記別の復号鍵変換データとを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録する。

【００５８】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからデータを再生する光ディスク再生装置において、上記光ディスクは、非暗号化領域と、暗号化領域とを含み、上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生する再生手段を備えたことを特徴とする。

【００５９】上記光ディスク再生装置において、好ましくは、上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、上記再生手段は、上記データの再生制御のために用いられる制御情報を制御情報記録セクタから再生し、上記制御情報に含まれる復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生する。また、上記光ディスク再生装置において、上記再生手段は、好ましくは、上記データ記録セクタの非暗号化領域に記録された別の復号鍵変換データを再生し、上記制御情報に含まれる復号鍵変換データと、上記再生された別の復号鍵変換データとを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生する。

【００６０】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクにデータを記録する光ディスク記録方法において、上記光ディスク

は、非暗号化領域と、暗号化領域とを含み、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録するステップを含むことを特徴とする。

【００６１】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからデータを再生する光ディスク再生方法において、上記光ディスクは、非暗号化領域と、暗号化領域とを含み、上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生するステップを含むことを特徴とする。

【００６２】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、データが記録されたデータ再生領域と、上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域とを含み、上記データ再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータが記録された領域を含むことを特徴とする。

【００６３】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、上記光ディスクは、データが記録されたデータ再生領域を含み、上記データ再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとが記録された領域を含むことを特徴とする。

【００６４】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域と、暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータが記録されたデータ再生領域と、上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとが記録されたキー管理情報領域とを含むことを特徴とする。

【００６５】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、上記光ディスクは、複数のセクタを備えたセクタ構造を有し、上記各セクタは、セクタヘッダ領域と、暗号化されたデータが記録されたメインデータ領域とを含み、上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも１つの復号鍵が記録された復号鍵情報領域を含み、上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする。

【0066】

【発明の実施の形態】以下、図面を参照して本発明に係る実施形態について説明する。

【0067】＜第1の実施形態＞図1は、本発明に係る第1の実施形態である記録型光ディスク100のデータ記録領域を示す平面図である。この記録型光ディスク100は、デジタルデータを記録することが可能な記録媒体であって、追記型光ディスクと、書き換え型光ディスクを含む。

【0068】図1において、101は光ディスク100の管理情報が記録されたリードイン領域、102は映画などの画像データ（静止画及び動画を含む。）や音楽などの音声データの少なくとも一方を含むAVデータのコンテンツや、コンピュータのソフトウェアなどの、著作権保護が必要なデジタルデータが記録されるユーザデータ領域、103は欠陥管理情報等が記録されるリードアウト領域である。リードイン領域101は、プリビットの形で記録された再生専用領域104と、ガイド溝を有する書き換え可能領域である記録再生領域106により構成される。ここで、再生専用領域104には、光ディスク100の物理特性を記述したコントロール領域などが製造業者によりプリビットの形式で記録される。リードアウト領域103や書き換え可能領域106には、光ディスク記録装置による書き込みテストのためのデータや光ディスク100上の欠陥を管理するための管理情報などが光ディスク記録装置により記録される。さらに、リードイン領域101の再生専用領域104の内周側には、ディスク個別情報としてBCA106は、以下に示すように公知の方法で、コンテンツが記録された光ディスク100が完成した後に、光ディスク100に追記される。

【0069】図2（a）は図1の光ディスク100のBCA106を形成するときの装置構成を示すブロック図及び縦断面図であり、図2（b）は図1の光ディスク100のBCA106を形成した後の光ディスク100の縦断面図及びその水平方向に対する反射光の強度を示すグラフである。図2（a）及び図2（b）では、両面記録型の光ディスク100の例を示しており、光ディスク100は、2つの基板201、207の間に、記録層202、反射層203、接合層204、反射層205及び記録層206が挿入されて構成される。

【0070】BCAを光ディスク100に記録するときにおいては、図2（a）に示すように、高パワーレーザー光源211からのレーザー光をフォーカスレンズ212を介して、例えば光ディスク100の反射層205にパルス状に照射して一部の反射層205を除去することにより、位相符号化変調（phase encoding modulation）したストライプ状のデータをビットに重ねて記録する。再生時には、図2（b）に示すように、反射層205が除去されている部分で反射光量が低下した信号が断続的に

再生され、再生された信号を2値化した後、位相符号化復調（phase encoding demodulation）することにより、BCAのデータを再生する。このような記録方式により作成されたBCAは、各光ディスク100等に固有な情報であるディスク識別子を記録することができ、さらに改ざんすることが不可能であるなどの特徴を有する。

【0071】図3は、図1のBCA106の記録フォーマットを示す図である。図3に示すように、BCA106には、同期コード301、エラー検出コード302、エラー訂正コード303などがBCAデータ304の読み取り率を改善するために記録される。これらの複数のBCAデータ304を連結することによって、ディスク識別情報306が構成される。ディスク識別情報306には、ユーザデータ領域へ記録可能なデータの種類の種別、ユーザデータ領域から再生可能なデータの種別が記録される。BCA106のデータは改ざんが不可能であるため、光ディスク100の製造時に記録されるディスク識別情報により利用者のディスク使用に一定の制限を与えることができる。

【0072】図4は、図1のユーザデータ領域102内のセクタデータ401のセクタ構造を示す図である。図4において、図1のユーザデータ領域102は、一定量の単位でアクセス可能なセクタ構造を有しており、そのセクタデータ401は、ヘッダ402、メインデータ403、エラー検出コード404により構成される。

【0073】ここで、メインデータ403は、AVデータやコンピュータのデータなどが記録される領域である。また、ヘッダ402には、データID（Data Identifier）405、IDエラー検出コード406、スクランブル制御情報407、キー情報408などが記録される。データID405には、セクタを識別するための論理アドレスなどが記録され、IDエラー検出コード406はデータIDのエラー検出するためのコードである。また、スクランブル制御情報407は、メインデータにスクランブルが施されているか否かを示すフラグであり、キー情報408はメインデータをデスクランブルするためのキーに関する情報が記録される。キーに関する情報としては、デスクランブルキーそのもの（第1の実施形態の変形例）や、光ディスク100上の別領域に記録したデスクランブルキーへのポインタであるキーインデックス（第1の実施形態）が記録される。図4の例では、光ディスク100上の別領域である図1のキー管理情報領域107に記録したデスクランブルキーを参照するためのキーインデックスが記録されている場合を示している。

【0074】図5は、図1のキー管理情報領域107の構成を示す図である。図5において、キー管理情報領域107は、キー情報領域501と、コンテンツ情報領域502と、キーインデックスリスト領域503とから構

成される。

【0075】キー情報領域501には、使用済みのデスクランブルキー領域の数504が記録されるとともに、キー情報領域501は、AVデータ等に施されたスクランブルを解くためのデスクランブルキーを記録する領域であるデスクランブルキー領域505と、デスクランブルキー領域505に記録されるデスクランブルキーの記録状態（未使用、領域予約済、記録済などを示す。）を記録するキーステータス領域506とを含む。デスクランブルキー領域505には複数のデスクランブルキーが記録され、デスクランブルキー領域505中での格納位置を表すキーインデックスがキーインデックスリスト領域503に記録され、上記複数のデスクランブルキーは当該キーインデックスにより参照可能である。キーステータス領域506には、先のデスクランブルキーの記録状態を表すステータス情報がキーインデックスで参照可能な位置に格納される。

【0076】コンテンツ情報領域502には、光ディスク100上に記録されるコンテンツの中で著作権保護が必要なものが登録され、それとともにコンテンツで利用されるキーに関する情報が登録される。コンテンツ情報領域502は、キーインデックスリスト領域503に登録されるコンテンツ数507と、コンテンツ数分のコンテンツ情報508が記録される。さらに、コンテンツ情報508には、コンテンツを識別するためのコンテンツIDと、そのコンテンツで利用されるデスクランブルキーの個数と、使用するキーを記録したキーインデックスリスト509へのポインタが記録される。キーインデックスリスト領域503は、コンテンツで使用するキーを参照するためのインデックスをコンテンツ単位でのリスト形式で記録する領域である。キーインデックスリスト領域503には、コンテンツで利用されている全デスクランブルキーの記録領域を参照するキーインデックスが記録される。

【0077】このように構成された記録型光ディスク100では、書き換えが困難なディスク識別情報にディスクの使用条件を表すような情報として、地域識別子、データカテゴリ識別子、ディスク識別子などを製造時に記録することにより、光ディスク記録再生装置でこれらの情報を検出し、コンテンツが持つ著作権の保護レベルや利用レベルに応じて記録動作及び再生動作を制御することを可能とする。また、書き換えが困難な方法によって記録されており利用者の側での変更ができないため、別の光ディスクに著作権保護されたコンテンツをコピーした場合でも、ユーザデータ領域はコピー可能であるが、ディスク識別情報はコピーすることはできない。従って、ディスク識別情報を用いてスクランブルしたデータを光ディスク上に記録しておくことで、異なるディスク識別情報を有する光ディスクではデスクランブルできないユーザデータ領域が存在し正しい再生ができない。

【0078】図15(a)は第1の実施形態においてコンテンツの記録時に地域識別子を記録する場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図であり、図15

(b)は第1の実施形態において地域識別子が光ディスクの出荷時に予め記録されている場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図である。

【0079】例えば、図15(a)に示すように、光ディスクの出荷時に地域識別コードが記録されておらず、コンテンツの記録時にコンテンツが利用可能な地域を表す地域識別子を記録及び再生領域に記録した場合には、他の地域での利用は防止できる。しかしながら、他の地域で使用すべきディスク（図15(a)中の地域RC2用）にもコンテンツの記録が可能であり、正しくコンテンツの再生が可能である。コンテンツのデジタルコピーが可能な記録媒体では、著作権者の利益を保護するために賦課金制度などが設けられ、光ディスクの販売時に料金に上乗せされて回収されている。しかしながら、上乗せされる賦課金は国毎に異なるため、他の国で利用されるべき記録媒体が不正に利用されると、本来、利益を得るべき著作権者に正しく配分されない可能性がある。

【0080】また、図15(b)に示すように、地域識別子が光ディスクの出荷時に予め改ざんできない方法により記録しておくことで、他の地域で利用されるべき光ディスクへのコンテンツのコピーや再生を防止することができる。同様に、データカテゴリ識別子をディスク識別情報として記録した場合には、記録するデータが有するカテゴリ識別子と比較することで、データを記録及び再生可能なディスクへのコンテンツのコピーや再生を制限できる。光ディスク毎に固有なディスク識別子をディスク識別情報として記録した場合には、記録するデータをディスク識別子で暗号化するなどして、その光ディスクでのみ利用可能とすることができる。

【0081】本実施形態において、ディスク識別情報によってスクランブルされるデータは、著作権保護が必要なAVデータやコンピュータデータでもよいし、AVデータやコンピュータデータに施されているスクランブルを解くためのデスクランブルキーでもよい。

【0082】図13は、第1の実施形態の変形例に係る、暗号化デスクランブルキーから正規のデスクランブルキーであるか否かを判定するための方法を示すブロック図である。図13に示すように、デスクランブルキーに、デスクランブルキーの誤りを検出するための誤り検出コードを付加したデータを、ディスク識別情報を用いてスクランブルすることにより計算した暗号化デスクランブルキーを光ディスクに記録してもよい。光ディスク再生装置では、暗号化デスクランブルキーをデスクランブルキーと誤り検出コードとに復号し、復号された誤り検出コードにおけるパリティチェックなどに基づいて誤

り検出することにより復号されたデスクランブルキーが正規のものであるかを判定する。例えば、異なるディスク識別情報によってデスクランブルした場合、誤ったデスクランブルキーが生成され、誤り検出コードをチェックすることにより、正規のデスクランブルキーでないことを判定できるので、不正なコピーを検出することができる。

【0083】なお、ディスク識別情報を記録する別の方法として複数種類のディスク識別情報をプリビットで作成したスタンプを用意しそれぞれから光ディスクを作成することによって、異なるスタンプから作成される光ディスク毎で異なる利用制限を与えるようにしてもよい。さらに、ディスク識別情報を、秘密鍵を用いてスクランブルしてスクランブルされたディスク識別情報を光ディスクに記録しておくことによって、ディスク識別情報に記述される著作権の保護レベルを利用者にわからなくし、その結果、著作権保護がより強化される。

【0084】図4において説明したキーに関する情報としてデスクランブルキーそのものを記録した場合（第1の実施形態の変形例）と、ディスク上の別領域に記録したデスクランブルキーへのポインタであるキーインデックスを記録した場合（第1の実施形態）について、図6（a）及び図6（b）を参照して説明する。ここで、図6（a）は第1の実施形態の変形例に係る、図1のセクタデータ401にデスクランブルキー及びAVデータを記録する記録方法を示すブロック図であり、図6（b）は第1の実施形態に係る、図1のセクタデータ401にデスクランブルキーへのキーインデックス及びAVデータを記録する記録方法を示すブロック図である。

【0085】図6（a）の場合においては、同一のセクタデータ401に、メインデータ403と、メインデータ403をデスクランブルするために必要なキー情報408aであるデスクランブルキーとを記録する。このため、AVデータの記録時には、デスクランブルに必要なデスクランブルキーを取得しておく必要がある。つまり、AVデータの記録時にキーそのものの入手や購入が不可欠である。

【0086】一方、図6（b）の場合では、同一のセクタデータ401に、メインデータ403と、メインデータ403をデスクランブルするために必要な情報を記録するデスクランブルキー領域を参照するキー情報408であるキーインデックスとを記録し、キーインデックスにて指定される領域にデスクランブルキーを記録する。AVデータの記録時には、記録するコンテンツで使用されるキーの中のどのキーでデータがデスクランブルできるのかを示すキーIDを取得し、コンテンツ情報に含まれるキーインデックスリストからキーIDに対応するキーインデックスであるキー情報408を取得し、メインデータ403とともに記録する。デスクランブルキーの記録はデスクランブルキーを入手した際に行われ、キー

IDに対応するキーインデックスにより示されるデスクランブルキー領域に記録される。この結果、AVデータとそれに対応するデスクランブルキーの記録は独立して行うことができる。つまり、AVデータの記録とキーの入手又は購入は独立に行うことができ、AVデータの記録時にキーの入手又は購入は必ずしも必要でなくなる。利用者はコンテンツを記録しておいて、実際に再生する際にキーを入手するという利用法が可能となる。

【0087】図14は、第1の実施形態の変形例に係る、デスクランブル領域管理テーブルの構成を示す図である。以上の実施形態においては、暗号化されたコンテンツとその暗号を解くためのデスクランブルキーを関連付けるために、同一セクタデータ401にデスクランブルキーを参照するためのキーインデックスを記録する場合について説明したが、暗号化されたコンテンツが記録されるセクタのアドレス範囲とデスクランブルキーとの対応関係を管理する図14のデスクランブル領域管理テーブルを用いてもよい。このデスクランブル領域管理テーブルでは、暗号化されたコンテンツが記録されるセクタのアドレス範囲が開始アドレスと終了アドレスで表され、それらのセクタのデータを再生する場合に、デスクランブルキーを参照し、暗号化されたコンテンツをデスクランブルする。

【0088】記録するコンテンツと、そこで使用されるデスクランブルキーを取得するために、コンテンツを識別可能とするコンテンツIDを利用する。図5に示したように光ディスク上に記録したコンテンツ情報領域502内のコンテンツ管理リストに記録されるコンテンツ情報中に、コンテンツIDとそのコンテンツで使用されるデスクランブルキーのリストとして記録される。1つのコンテンツに対して複数のデスクランブルキーを使用できるようにリスト構成を取ることによって、一部のコンテンツやソフトウェアの切り売りするようなサービスが可能となる。

【0089】また、図13を参照して上述した変形例においては、チェックサムや巡回冗長検査符号などのエラー検出コードが付加されたデスクランブルキーをディスク識別情報でスクランブルしたデータを他のディスクへ不正にコピーした場合には、異なるディスク識別情報でデスクランブルを行うことによりエラーとして検出される。このような場合に、このデスクランブルキーを光ディスク上に記録されているディスク識別情報によってスクランブルされたデスクランブルキーを入手し、それに置きかえることによって正しく再生できるようなディスクを作成することもできる。

【0090】図1のキー管理情報領域107は書き換え可能なリードイン領域101に記録される。通常、ユーザデータ領域102はパーソナルコンピュータのドライブ装置からアクセス可能なユーザ領域と、光ディスク上の欠陥セクタに対するスベア領域とからなり、通常の読

み出しコマンドや書き込みコマンドでは、ユーザ領域のみが論理的な連続領域としてアクセス可能である。キー管理情報をリードイン領域101に配置することにより、パーソナルコンピュータのドライブ装置などから直接アクセスされることを防止し、パーソナルコンピュータからAVデータ等に施されたスクランブルを解くためのキーの取得を不可能とすることができる。

【0091】<第2の実施形態>図7は、本発明に係る第2の実施形態である光ディスク記録再生装置の構成を示すブロック図である。この光ディスク記録再生装置は、第1の実施形態に係る光ディスク100に著作権保護を必要とする画像データや音楽データなどのAVデータのコンテンツを記録する装置である。

【0092】図7において、701は第1の実施形態の光ディスク、702は半導体レーザと光学素子から構成される光ピックアップである光ヘッド、703は半導体レーザの動作制御及び再生信号の2値化を行う記録再生制御回路、704は記録すべきデジタルデータをデジタル変調するとともに2値化された再生信号をデジタル復調する変復調回路、705は光ディスク701上の傷や埃等で生じたエラーの誤り検出及び訂正処理と、誤り検出及び訂正処理に必要な誤り訂正コードの生成処理を行う誤り検出及び訂正回路、706は誤り検出及び訂正回路705の作業用メモリ及びデータバッファメモリとして用いるRAMであるバッファメモリ、707はスクランブルされて記録されているAVデータをデスクランブルするデスクランブル回路、708は圧縮されて記録された動画データ等を伸長するMPEG復号回路、709は伸長された画像データをD/A変換してビデオ信号及びオーディオ信号を生成して出力する出力回路、710は光ディスク記録再生装置全体の動作を制御する制御CPU、711はコンテンツに施された暗号を解くデスクランブルキーを取得する通信回路、712はセットトップボックスなどの通信端末装置から画像データや音楽データなどの暗号化されたコンテンツのデジタルデータを受信するデータ受信回路である。

【0093】以上のように構成された、図7の光ディスク記録再生装置におけるデータ記録動作について説明する。セットトップボックスやMPEGエンコーダなどの通信端末装置から送信されてきた画像データや音楽データなどの暗号化されたコンテンツのデジタルデータはデータ受信回路712によって受信された後、バッファメモリ706に一時的に保存される。誤り検出及び訂正回路705は、保存されたコンテンツのデジタルデータに、光ディスク701の傷や埃等に起因する誤りの検出及び訂正処理に必要な誤り検出及び訂正コードを生成し、記録データを再構成する。誤り検出及び訂正コードには、例えば公知のリードソロモン符号などの符号が用いられる。ここで、再構成された記録データは、コンテンツのデジタルデータと、誤り検出及び訂正コードと

を含む。変復調回路704は、記録の際に8/16変調方式などの変調方式を用いて、記録データをデジタル変調する。そして、記録再生制御回路703は、デジタル変調された記録データに従って、光ヘッド702から出力されるレーザ光のパワーを強度変調して、当該レーザを光ディスク701に照射することにより、記録データを光ディスク701上に記録する。

【0094】図8は、図7の光ディスク記録再生装置の制御CPU710によって実行されるAVデータの記録処理を示すフローチャートである。

【0095】図8において、まず、ステップS801において、光ディスク701からのAVデータの記録に先立ち、リードイン領域101のディスク識別情報を再生し、次いで、ステップS802において、ディスク識別情報に記録されている、ユーザデータ領域102に記録可能なデータの種別から、現在記録しようとしているコンテンツのデジタルデータが記録可能であるか否かを判断する。ステップS802でYESのときはステップS803に進む一方、NOであるときはステップS810で記録動作を中止して当該AVデータの記録処理を終了する。

【0096】ステップS803では、リードイン領域101においてキー管理情報が記録されたセクタのデータを再生し、ステップS804では、再生したキー管理情報にコンテンツの記録に必要なキー情報に対する領域が割り当て済みであるか否かを判断する。ステップS804でNOであるときは、キー管理情報領域107にキー情報を記録するための領域を割り当てた後、ステップS806に進む。一方、ステップS804でYESのときはそのままステップS806に進む。

【0097】コンテンツの記録を行う場合には、光ディスク記録再生装置の制御CPU710は、記録する暗号化されたコンテンツのデータと、暗号を解くためのデスクランブルキーに関する情報を、通信端末装置からデータ受信回路712を介して受信する。ここで、キーに関する情報とは、コンテンツで使用されるキーそのもの、もしくは、コンテンツ全体で使用するキーのうち何番目のキーに対応するのかわかるキーIDである。キーIDを受信した場合に、ステップS806では、受信されたキーIDを、キーIDに対応するデスクランブルキーが記録されている領域を示すポインタであるキーインデックスに変換し、変換されたデスクランブルキーを、そのデスクランブルキーで復号されるコンテンツのデータが記録されるセクタのヘッダ領域に配置される。そして、ステップS807では、制御CPU710は、記録再生制御回路703と、変復調回路704と、誤り検出及び訂正回路705とを制御することにより、以下の記録データに対してエラー検出及び訂正用のコードを付加し、これらのコードが付加されたセクタデータを、公知

の8/16変調方式などの変調方式を用いてデジタル変調し、所定の記録位置に光ヘッド702を制御するとともに、デジタル変調された記録データに従ってレーザ光を強度変調する。これによって、記録データを光ディスク701上に記録する。さらに、ステップS808では、コンテンツの記録の終了であるか否かを判断し、NOであるときはステップS806に戻り、上記の処理を繰り返す。ステップS808でYESであれば、ステップS809で、更新されたキー管理情報を光ディスク701上のキー管理情報領域107に記録して当該AVデータの記録処理を終了する。

【0098】図9は、図7の光ディスク記録再生装置の制御CPU710によって実行されるキー管理情報領域の割り当て処理を示すフローチャートである。この処理は、コンテンツのデータの記録に先立ち、デスクランブルキーを記録するための領域を割り当てる処理である。

【0099】図9において、まず、ステップS901において、例えば電子プログラムガイド等から記録するコンテンツのキーに関する情報（使用するデスクランブルキーの個数などを含む。）を取得し、次いで、ステップS902では、光ディスク701に記録されているキー管理情報領域107内のキー管理情報を再生し、ステップS903において、デスクランブルキー領域605の空き領域をキーステータス領域606から調べ、記録しようとしているコンテンツで使用するデスクランブルキーを記録できるか否かを判定する。ステップS903でNOであるときは、ステップS907で記録動作を中止して当該割り当て処理を終了する。一方、ステップS903でYESであるときは、ステップS904で、記録するコンテンツをコンテンツ情報領域502内のコンテンツリストに登録し、ステップS905においてデスクランブルキー領域605に対して、デスクランブルキーの記録に必要な領域を予約するために、対応するキーステータス領域に領域予約済みフラグを設定することにより記録用領域を割り当てる。さらに、ステップS906で、デスクランブルキーを記録するために割り当てられた領域を示すキーインデックスをキーリストとして作成し、コンテンツ情報としてのポインタを割り当てた後、当該割り当て処理を終了する。

【0100】図10は、図7の光ディスク記録再生装置の制御CPU710によって実行されるデスクランブルキーの記録処理を示すフローチャートである。この記録処理は、キー管理センターからデスクランブルキーを取得して光ディスク701に記録するための処理である。

【0101】図10において、まず、ステップS1001において、光ディスク701のリードイン領域101のディスク識別情報を再生した後、ステップS1002において、キー管理センターからデスクランブルキーを取得するために、ディスク識別情報と、所望のコンテンツのデスクランブルに必要なキーを識別するためのキー

IDを通信回路711を介してキー管理センターに送信する。キー管理センターでは、与えられたキーIDからコンテンツのデスクランブルに必要なデスクランブル鍵を選択し、送られてきたディスク識別情報等の情報によって、デスクランブルキーを暗号化して返信する。

【0102】ステップS1003で、キー管理センターから通信回路711を介して、キーIDに対応するデスクランブルキーを取得した後、ステップS1004で、キー管理情報領域107のデータを再生し、再生されたキー管理情報領域107内のデータのうちキーIDで示されるキーインデックスリストから、デスクランブルキーを記録する領域を示すキーインデックスを取得する。次いで、ステップS1005において、キーインデックスにより示されたデスクランブルキー領域に上記取得したデスクランブルキーを配置し、対応するキーステータス領域606にキー取得済みを示す取得済みフラグを設定する。さらに、ステップS1006で、すべてのキーの取得が終了したか否かが判断され、NOであれば、ステップS1003に戻り上記の処理を繰り返す。一方、ステップS1006でYESであるときは、ステップS1007において、更新されたキー管理情報をキー管理情報領域107に記録して当該デスクランブルキーの記録処理を終了する。

【0103】次いで、本実施形態の光ディスク記録再生装置のデータ再生動作について図7を参照して説明する。光ディスク701に記録されたデジタルデータは、以下のようにして再生される。光ヘッド702の半導体レーザからのレーザ光は光ディスク701に照射され、そのときに光ディスク701で反射される反射光が光ヘッド702を介して記録再生制御回路703に入射する。記録再生制御回路703は、入射する反射光を光電変換した後、増幅及び2値化処理を実行することにより、デジタル化された再生信号を生成して変復調回路704に出力する。変復調回路704は、記録の際に公知の8/16変調方式などの変調方式を用いてデジタル変調された信号をデジタル信号にデジタル復調して、誤り検出及び訂正回路705に出力する。次いで、誤り検出及び訂正回路705は、バッファメモリ706を作業用メモリとして用いて、光ディスク701の傷や埃など起因する誤りの検出及び訂正処理を実行する。この誤り検出及び訂正処理は、例えば、既知のリードシロモン符号などの復号を行うことで実行される。

【0104】誤り検出及び訂正処理された再生データは、デスクランブル処理を行うために、デスクランブル回路707に出力される。デスクランブル回路707は、予めデータの再生に先立って再生したキー管理情報領域107のデスクランブルキーを用いて再生データにデスクランブル処理を施した後、MPEG復号回路708に出力する。次いで、MPEG復号回路708は、圧縮された動画データや音楽データを伸長した後、伸長後

のデータを出力回路709に出力する。さらに、出力回路709は、入力される伸長されたデータをビデオ信号及びオーディオ信号にD/A変換して、テレビジョン装置やオーディオ機器などの上位の機器に出力する。

【0105】図11は、図7の光ディスク記録再生装置の制御CPU710によって実行されるAVデータの再生処理を示すフローチャートである。図11において、まず、ステップS1101において、光ディスク701からのAVデータの記録に先立ち、リードイン領域101内のディスク識別情報を再生し、ステップS1102において、ディスク識別情報に記録されている再生可能なデータの種別から、現在再生しようとしているコンテンツが再生可能であるか否かを判断する。ステップS1102でNOであるときは、ステップS1112で再生動作を中止して当該AVデータの再生処理を終了する。一方、ステップS1102でYESであるときは、ステップS1103で、リードイン領域101のキー管理情報領域107内でキー管理情報が記録されたセクタのデータを再生し、ステップS1104において再生したキー管理情報において、コンテンツの再生に必要な情報が記録済みであるか否かを判断する。ステップS1104でYESであるときはそのままステップS1106に進む一方、NOであれば、ステップS1105において、キーを管理しているキー管理センターから通信回路711を介してデスクランブルキーを取得し、光ディスク701のキー管理情報領域107に記録してステップS1106に進む。

【0106】次いで、ステップS1106では、制御CPU710は、光ディスク701のユーザデータ領域に光ヘッド702を移動させ、記録再生制御回路703、変復調回路704、誤り検出及び訂正回路705を制御してAVデータを再生する。そして、ステップS1107では、再生されたセクタのヘッダに含まれるキーインデックスにより示されるデスクランブルキー領域606から、セクタデータのデスクランブルに必要なデスクランブルキーを取得し、ステップS1108では、デスクランブルキーに対して行われているスクランブルを、ディスク識別情報によってデスクランブルすることにより復号する。さらに、ステップS1108において、デスクランブルキーに付与されているエラー検出コードをチェックすることにより、デスクランブルキーに誤りがあるか否かを判断する。ステップS1108でYESであるときは、不正に入手したコンテンツ（又は不正にコピーしたコンテンツ）とみなし、ステップS1112で再生動作を中止して当該AVデータの再生処理を終了する。

【0107】一方、ステップS1108でNOであるときは、S1109において、デスクランブルキーによりコンテンツのデータをデスクランブルし、ステップS1110において、デスクランブルされたAVデータをM

PEG復号回路708に出力する。そして、制御CPU710は、MPEG復号回路708及び出力回路709を制御することにより、デスクランブルされたAVデータをMPEG伸長した後、ビデオ信号とオーディオ信号にD/A変換してテレビジョン装置やオーディオ機器などの上位機器に出力する。次いで、ステップS1111では、コンテンツの再生の終了か否かが判断され、NOであるときはステップS1106に戻り、上記の処理を繰り返す。一方、ステップS1111でYESのときは当該AVデータの再生処理を終了する。

【0108】なお、ステップS1109で誤りが検出された場合には、不正に入手したコンテンツとみなし、例えば、不正にコピーしたコンテンツとみなし、再生動作を中止したが、キーが記録されていない場合と同様に、ステップS1105の処理を実行することにより、通信回路711を介して、キーを管理しているキー管理センターからキー情報を取得し、光ディスク701のキー管理情報領域107に記録してもよい。これにより、コピーしたAVデータであっても、キーを正規に入手することによって再生可能にすることができる。

【0109】図12は、図7の光ディスク記録再生装置の制御CPU710によって実行されるデスクランブルキーの取得処理を示すフローチャートである。この処理は、再生されたキーインデックスからデスクランブルキーを再生する処理であり、図11に図示されたAVデータの再生処理に先立って実行される。

【0110】図12において、まず、ステップS1201では、再生されたセクタ領域のデータがスクランブルされているか否かをスクランブル制御情報により判断し、NOであるときはステップS1206に進む一方、YESであるときは、ステップS1202において上記セクタ領域と同一のセクタ領域内に記録されているキー情報を再生することによりキーインデックスを取得し、次いで、ステップS1203においてデスクランブルキー領域606から上記キーインデックスによって示されるデスクランブルキーを取得した後、ステップS1204では、取得されたデスクランブルキーをディスク識別情報を用いてデスクランブルし、エラー検出コードを調べることでデスクランブルキーが誤りがあるか否かを判断する。ステップS1204でYESのときは、ステップS1205で再生動作を中止して当該デスクランブルキーの取得処理を終了する。一方、ステップS1204でNOであるときは、ステップS1206に進む。再生されたセクタがスクランブルされていない場合やデスクランブルキーをディスク識別情報によってデスクランブルされた結果に誤りがない場合には、ステップS1206において再生動作の許可を行い、再生されたセクタのデータを出力して当該デスクランブルキーの取得処理を終了する。

【0111】以上説明したように、本発明に係る実施形

態の光ディスク及び光ディスク記録再生装置では、ディスク製造段階で作成された再生専用のディスク識別情報を用いて利用者による記録や再生動作を制御することができる。さらに、上記のディスク識別情報を用いてデータの一部をスクランブルすることにより、ユーザデータ領域の物理コピーが行われたディスクに対して正常に再生すること防止することができる。また、データのデスクランブルに必要なデスクランブルキーをデータとは別領域に配置することにより、コンテンツの記録とデスクランブルキーの記録を独立に行うことができる。このため、コンテンツを記録しておき、必要に応じて、例えばコンテンツのデータの再生時に、デスクランブルキーを取得することにより、コンテンツの再生可能な状態とすることができる。この際、デスクランブルキーをディスク識別情報によりスクランブルしておくことで、上述した場合と同様に、物理的なコピーによる不正な利用を防止できることは明らかである。それに加えて、不正にコピーしたディスクであっても、その光ディスクのディスク識別情報でスクランブルされたデスクランブルキーを正式にキー管理センターから取得し、光ディスクに記録することにより、正しく再生できる光ディスクにすることもできる。

【0112】なお、光ディスク記録再生装置に入力されるコンテンツのデータについて既に暗号化されたものについて説明したが、光ディスク記録再生装置内にコンテンツを暗号化する回路を備えることで、入力されたコンテンツのデータを暗号化し、光ディスク上に記録することにより同様の効果が得られる。

【0113】また、本実施形態では、暗号化されたコンテンツの解読に必要なデスクランブルキーのみをディスク識別情報を用いて暗号化することにより、異なるディスク識別情報を有するディスク間でのコピーの防止を行ったが、コンテンツ自身にディスク識別情報を用いた暗号化を施すことにより、同様にコピーの防止を行うことができる。さらに、ディスク識別情報にも秘密鍵を用いて暗号化を施すことにより、ディスク上に記録されたコンテンツの不正な解読をより困難にすることができる。

【0114】＜第1及び第2の実施形態の効果＞本発明に係る実施形態の光ディスクは、ユーザデータ領域への記録動作や再生動作を光ディスク毎に行うディスク識別情報が書き換え不可能な再生専用領域に記録されることにより、利用者による光ディスク上へのコンテンツの記録動作や再生動作を光ディスクの製造時に記録する情報を用いて制御することができる。

【0115】本発明に係る実施形態の光ディスクは、書き換えが不可能な再生専用のディスク識別情報を鍵として暗号化されたデータが光ディスク上のユーザデータ領域に記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい

復号並びに再生が不可能とすることができる。

【0116】本発明に係る実施形態の光ディスクは、暗号化されたデータと暗号を解くデスクランブルキーとが異なるセクタ領域に記録されることにより、映画や音楽などの著作権保護が必要なデータの取得と暗号を解くためのデスクランブルキーの取得を独立に行うことが可能となる。さらに、ディスク識別情報を鍵としてデスクランブルキーを暗号化して記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とし、コピー先の光ディスクのディスク識別情報を鍵として暗号化したデスクランブルキーを取得し記録することで、データの正しい復号並びに再生を可能とすることができる。

【0117】＜第3の実施形態＞次いで、本発明に係る第3の実施形態である暗号化コンテンツ記録及び再生方法について図面を参照しながら説明する。図16は、本発明に係る第3の実施形態である光ディスク1101のデータ記録領域を示す平面図である。

【0118】図16において、1101はデジタルデータを記録することが可能な記録媒体であって、書き換え型又は追記型の光ディスクである記録型光ディスク、1102はディスク情報が微小な凹凸ピットの形式で記録されたコントロールユーザデータ領域、1103はレーザ光の光ビームを光ディスクに照射することによりユーザがデータを記録するユーザデータ領域、1104はディスク1Dが記録されたBCAである。BCA1104において、コントロールユーザデータ領域1102の内周部分の微小な凹凸ピット上の記録膜は、半径方向に長い形状でかつ複数個のトリミング領域1105が形成されるように、その記録膜に対して部分的にYAGレーザなどのパルスレーザのレーザ光を放射することによりトリミングされ、これによりデスクランブル識別情報であるディスク1Dが記録される。

【0119】図17は、第3の実施形態に係るBCA再生回路1401における再生信号1201及び再生2値化信号1207の信号波形を示す波形図であり、図18は、第3の実施形態に係るBCA再生回路1401の構成を示すブロック図である。図17において、BCA1104のデータを再生したときの再生信号1201を示している。図18において、1301は光ピックアップ、1302はプリアンプ、1303は低域通過フィルタ(LPF)、1304は2値化回路、1305は復調回路である。

【0120】図18において、光ピックアップ1301から出力されるレーザ光は光ディスク1101のBCA1104を照射し、その反射光は光ピックアップ1301により光電変換された後、光電変換後の電気信号は、プリアンプ1302で増幅されて再生信号1201が得

られる。ここで、図17の再生信号1201はコントロールユーザデータ領域1102の凹凸ビットに応じたレベルを有する信号であり、この再生信号1201において、1202、1203、1204はパルスレーザによるトリミング処理により記録膜が取り除かれて、凹凸ビットによる信号が欠落しているトリミング部分である。このトリミング処理は、光ディスクの製造者によって行われる。

【0121】図18に戻り説明すると、再生信号1201は低域通過フィルタ1303に入力されて、凹凸ビットによる変調信号が除去された後に、2値化回路1304に入力される。2値化回路1304に入力された再生信号は、コントロールユーザデータ領域1102の信号を2値化する通常のスライスレベル1205ではなく、スライスレベル1205よりも十分に低いレベルであるスライスレベル1206を用いて2値化されて、再生2値化信号1207が得られる。2値化回路1304から出力される再生2値化信号1207は、復調回路1306で復調されてディスクID信号1306が得られる。

【0122】以上説明したように、光ディスクを識別するディスク識別情報を付加することにより、光ディスクの管理を容易に実現することができる。また、BCA1104が凹凸ビット上に記録されることにより、BCA1104内の光ディスクを識別する情報が容易に改ざんされることを防止することができる。さらに、図16のコントロールユーザデータ領域1102とBCA1104が隣接していることにより、コントロールユーザデータ領域1102のデータを再生する際に、BCA1104のデータも読めて再生することができ、もしくはBCA1104のデータを再生する際に、コントロールユーザデータ領域1102のデータを読めて再生することができるので、例えば光ディスクを起動する際にCPUが速やかに光ディスクを識別するためのBCA1104の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【0123】なお、本実施形態のBCA1104は、コントロールユーザデータ領域1102の内周部分の凹凸ビット上の記録膜をトリミングすることにより形成されているが、書き換え型又は追記型の光ディスクである記録形光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールユーザデータ領域1102の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からユーザデータ領域1103を保護することができる。また、コントロールユーザデータ領域1102の内周側にBCA1104を形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する際のマージンを考慮しているためである。

【0124】なお、トリミング前のBCA1104に記

録されているデータが、コントロールユーザデータ領域1102に記録されていてもよい。BCA1104に記録されているデータが、コントロールユーザデータ領域1102にも記録されていることにより、トリミングを行ってもコントロールユーザデータ領域1102の上記データを保護することができる。さらに、BCA1104に記録されているデータが、BCA1104から、コントロールユーザデータ領域1102まで連続して繰り返し記録されている場合には、コントロールユーザデータ領域1102の上記データを見つけることによって、BCA1104の位置を予想することができる。

【0125】次いで、上記BCA1104を有する光ディスク1101に、ネットワークを介して、ディスクIDで暗号化されたコンテンツを記録する手順を述べる。第3乃至第5の実施形態において、ネットワークとは、例えば、インターネット、公衆電話回線、又は専用線などの通信網をいう。図19は、第3の実施形態に係る光ディスク記録再生システムの構成を示すブロック図であり、上記BCA1104を有する書き換え型又は追記型の光ディスクである記録型光ディスク1101に暗号化コンテンツを記録する装置構成を示す。

【0126】図19において、光ディスク記録再生システムは、互いにインターネットなどのネットワーク1405を介して接続された、光ディスク記録再生装置1410と、暗号化部1406とを備えて構成される。光ディスク記録再生装置1410は、光ピックアップ1301と、BCA再生回路1401と、インターネット403と、記録回路1411と、データ再生部1412と、暗号デコーダ1413とを備える。また、暗号化部1406は、インターフェース1404と、コンテンツメモリ1407と、暗号化エンコーダ1408とを備える。

【0127】まず、光ピックアップ1301から出力されるレーザ光は、例えばRAM型光ディスク1101のBCA1104を照射し、その反射光は光ピックアップ1301によって光電変換された後、光電変換された再生信号がBCA再生回路1401に入力される。BCA再生回路1401は入力された再生信号に基づいてBCA内のディスクID信号1402を再生して、再生されたディスクID信号1402を暗号デコーダ1413に出力するとともに、インターフェース1404及び1404とネットワーク1405を介して、暗号化部1406の暗号化エンコーダ1408に送られる。暗号化エンコーダ1408は、コンテンツメモリ1407内のコンテンツのデータが記録される光ディスク1101のディスクID信号1402が暗号を解く復号鍵となるように、当該コンテンツのデータを暗号化し、又は画像音声用のスクランブルを行う。

【0128】なお、本実施形態では、暗号化処理について、コンテンツ1407を、ディスクID信号1402を暗号鍵として用いて暗号化すると表現しても同一の意

味とする。また、本実施形態においては、暗号化や復号化を、錠と鍵の関係で考え、上記錠を上記鍵で閉めることを暗号化とし、上記錠を上記鍵で開けることを復号化とする。従って、暗号化と復号化で実際の演算は異なるが、暗号化するための錠と復号化するための錠は、同一であるとする。なお、コンテンツ1407をCとし、ディスクID信号1402をBCASとし、暗号化されたコンテンツ1409をC[BCAS]とし、暗号化処理の演算を*で表し、次式のように表記する。

【0129】

【数1】 $C * BCAS = C [BCAS]$

【0130】暗号化部1406によって暗号化されたコンテンツ1409は、インターフェース1403及び1404とネットワーク1405を介して記録再生装置1410の記録回路1411に送られる。記録回路1411は、入力されるコンテンツのデータを所定のデジタル変調し、デジタル変調されたデータに応じて光ピックアップ1301からのレーザ光を強度変調して光ディスク1101に照射することにより、コンテンツのデータを光ディスク1101に記録する。

【0131】次に、光ディスク1101に暗号化されて記録された上記コンテンツを再生する際は、光ピックアップ1301から出力されるレーザ光がユーザデータ領域1103の上記暗号化コンテンツが記録された領域を照射し、その反射光が光ピックアップ1301によって光電変換された後、光電変換された再生信号がデータ再生部1412に入力される。データ再生部1412は、入力された再生信号をデジタルデータにA/D変換して暗号デコーダ1413に出力する。一方、光ピックアップ1301からのレーザ光は光ディスク1101のBCA1104を照射し、その反射光は光ピックアップ1301によって光電変換された後、光電変換された再生信号はBCA再生回路1401に入力される。BCA再生回路1401は入力された再生信号をA/D変換してディスクID信号1402を発生して、当該ディスクID信号を暗号デコーダ1413に出力する。

【0132】暗号デコーダ1413は、入力されたディスクID信号1402を鍵として用いて、暗号化されたコンテンツのデータを復号する。このとき、コンテンツが正規に光ディスク1101に記録されている場合は、光ディスク1101に記録されている暗号化コンテンツを復号するための錠は、光ディスク1101のディスクID信号1402であり、再生時にBCA再生回路1401から出力されるディスクID信号1402も、光ディスク1101のディスクID信号(BCAS)である。従って、復号又はデスクランブルされたコンテンツが暗号デコーダ1413から出力信号1414として出力される。なお、復号化処理の演算を#とすると、次式のように表記される。

【0133】

【数2】 $C [BCAS] \# BCAS = C$

【0134】ここで、コンテンツのデータが画像データの場合は、例えばMPEG信号のデータが伸長されて、画像信号のデータが得られる。

【0135】以上説明したように、本実施形態における暗号化は、ディスクIDを鍵としており、ディスクIDは、1枚の光ディスクに対応して1個しか存在しないため、当該1枚の光ディスクにしか同一の暗号化コンテンツの記録をすることができないという効果がある。すなわち、上記コンテンツ1407を、例えばID1というディスクIDを持つ正規の光ディスクから、ID2という別のディスクIDを持つ別の光ディスクにコピーして再生しようとした場合、BCA再生回路401からディスクID信号1402としてID2が出力される。しかしながら、暗号化コンテンツはID1というディスクID信号で暗号化されているので、暗号デコーダ1413で、暗号化コンテンツを復号することができない。

【0136】なお、暗号化エンコーダ1408はコンテンツの供給元ではなく、ネットワークに対して記録再生装置側にあり、暗号化エンコーダを搭載したICカードなどの形態であってもよい。また、上記光ディスク1101はディスクIDのみで暗号化されているので、BCA再生回路1401と暗号デコーダ1413を有する任意の光ディスク記録再生装置で再生することが可能である。

【0137】<第4の実施形態>次いで、本発明に係る第4の実施形態である暗号化コンテンツ記録方法について図面を参照しながら説明する。図20は、本発明に係る第4の実施形態である光ディスク記録再生システムの構成を示すブロック図であり、BCAを有する書き換え型又は追記型光ディスクである記録型光ディスクに、暗号化コンテンツを記録する装置構成を示す。なお、第4の実施形態の説明において、第3の実施形態と共通の部分はその説明を簡略化する。

【0138】図20において、第4の実施形態に係る光ディスク記録再生システムは、CATV会社装置1501と、鍵発行センター装置1507と、CATVデコーダ1506と、光ディスク記録再生装置1514と、テレビジョン装置1530とを備えて構成される。ここで、CATV会社装置1501は、映画ソフトウェアなどのコンテンツのデータを格納するコンテンツメモリ1502と、第1暗号鍵を格納する第1暗号鍵メモリ1503と、第1暗号化エンコーダ1504とを備える。また、鍵発行センター装置1507は、その装置1507の動作を制御する制御部1507aと、時間制限情報を格納する時間制限情報メモリ1510と、記録許可コードを格納する記録許可コードメモリ1511とを備える。さらに、CATVデコーダ1506は、CATVデコーダ1506のシステムIDを格納するシステムIDメモリ1508と、第1暗号デコーダ1513と、第2

暗号化エンコーダ1516と、ICカード1522内の会社識別番号メモリ1523とを備える。またさらに、光ディスク記録再生装置1514は、記録回路1518と、データ再生部1519と、BCA再生回路1521と、第2暗号デコーダ1520と、ICカード1524内の会社識別番号メモリ1526とを備える。

【0139】まず、CATV会社装置1501の第1暗号化エンコーダ1504は、映画ソフトウェアなどのコンテンツメモリ1502内のコンテンツのデータを第1暗号鍵1503を用いて暗号化することにより、第1暗号化コンテンツ1505を生成し、生成された第1暗号化コンテンツ1505をネットワークを介して各ユーザのCATVデコーダ1506の第1暗号化デコーダ1513に送信する。ここで、コンテンツメモリ1502内のデータをCとし、第1暗号鍵1503をFKとし、第1暗号化コンテンツ1505をC[FK]とすると、次式のように表記される。

【0140】

【数3】 $C * FK = C[FK]$

【0141】CATVデコーダ1506は、システムIDメモリ1508内の当該CATVデコーダ1506のシステムIDと、視聴もしくはRAM型光ディスク1101への記録を行いたい上記コンテンツに予め付与され、例えば当該CATVデコーダ1506のキーボード（図示せず。）を用いて入力されたタイトルコード1509とを、ネットワークを介して鍵発行センター装置1507に送信する。ここで、タイトルコード1509はTVの画面に従って選択することにより入力してもよいし、直接にキーボードから入力してもよいし、リモートコントローラー等から入力してもよい。従って、タイトルコード1509は、ユーザが独自に入手していてもよいし、第1暗号化コンテンツ1505とともにCATVデコーダ1506に送られてきててもよいし、番組案内などの形態で第1暗号化コンテンツ1505とは別の時刻に予め送られていてもよい。

【0142】鍵発行センター装置1507の制御部1507aは、CATVデコーダ1506のシステムIDと、上記コンテンツのタイトルコード1509とに基づいて、時間制限情報メモリ1510内の時間制限情報と、記録許可コードメモリ1511内の記録許可コードとを参照して、これらに対応する鍵(K)1512を記録許可コード及び時間制限コードとともにCATVデコーダ1506の第1暗号デコーダ1513に対して、ネットワークを介して送信する。なお、時間制限情報により、同一のコンテンツを時刻を変えて複数回放送する場合を区別することができる。ここで、第1復号鍵をFKとし、CATVデコーダ1506のシステムIDをDIDとし、時間制限情報をTIMEとし、記録許可コードをCOPYとし、コンテンツのタイトルコード1509をTとすると、鍵(K)は、次式の関係を満たしてい

る。

【0143】

【数4】 $FK = K * T * DID * TIME * COPY$

【0144】なお、記録許可コードメモリ1511内の記録許可コードは、例えばCATV会社装置1501が、放送するコンテンツが新作品か旧作品かを判断して、視聴のみ許可するのか、視聴、記録の両方を許可するのかを決定する。

【0145】CATVデコーダ1506の第1暗号デコーダ1513は、第1復号鍵(FK)と、鍵(K)1512と、上記コンテンツのタイトルコード1509と、システムIDと、記録許可コードと、時間制限情報とが上述の関係を満たしており、かつクロック回路1527から出力される現在時刻情報が当該時間制限情報の条件を満たしていれば、第1暗号化コンテンツ1505を復号する。ここで、上記暗号化されたコンテンツが画像信号の場合は、デスクランブルされた画像信号が第1暗号化デコーダ1513からテレビジョン装置1530に出力されて視聴できる。ここで、第1暗号化デコーダ1513の復号化処理は次式で表される。

【0146】

【数5】

$C[FK] \# (K * T * DID * TIME * COPY) = C[FK] \# FK = C$

【0147】なお、記録許可コードが視聴のみ許可する場合は、光ディスク1101に記録できないが、視聴と記録の両方を許可する場合は記録することができるので、以下でこの方法について説明する。

【0148】光ディスク記録再生装置1514のBCA再生回路1521は、光ディスク1101のBCA1104のデータを再生してディスクID信号1515を得て、当該ディスクID信号をCATVデコーダ1506の第2暗号化エンコーダ1516に出力する。CATVデコーダ1506の第2暗号化エンコーダ1516は、ディスクID信号1515を第2暗号鍵として用いて、第1暗号デコーダ1513から出力されたコンテンツのデータを暗号化することにより、第2暗号化コンテンツ1517を生成して光ディスク記録再生装置1514の記録回路1518に送信する。なお、第2暗号デコーダ1516の上記暗号化は、第1暗号デコーダ1513から第1暗号化コンテンツが復号されて出力されている時間に限られる。ここで、第1暗号デコーダ1513の出力信号であるコンテンツをCとし、第2暗号鍵であるディスクID信号1515をBCASとし、第2暗号化コンテンツ1517をC[BCAS]とすると、次式のように表記される。

【0149】

【数6】 $C * BCAS = C[BCAS]$

【0150】光ディスク記録再生装置1514の記録回

路1518に送られた第2暗号化コンテンツ1517は、記録回路1518により、例えば公知の8/16変調方式により変調されて、光ピックアップ（図示せず。）により光ディスク1101のユーザデータ領域1103に記録される。光ディスク1101に暗号化されて記録された上記コンテンツを再生する際は、光ピックアップから出力されるレーザ光が光ディスク1101の上記暗号化されたコンテンツが記録されている領域を照射し、その反射光が光ピックアップに入射する。上記光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をデータ再生部1519に出力し、データ再生部1519は、入力された再生信号をデジタル再生信号にA/D変換して第2暗号デコーダ1520に出力する。

【0151】一方、光ピックアップから出力されるレーザ光は光ディスク1101のBCA1104を照射し、その反射光が光ピックアップに入射する。上記光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をBCA再生回路1521に出力する。BCA再生回路1521は入力された再生信号に基づいてディスクID信号1515を生成して第2暗号デコーダ1520に出力する。これにตอบสนองして、第2暗号デコーダ1520は、入力されたディスクID信号1515を鍵として用いて、データ再生部1519から出力される再生された暗号化コンテンツの復号を行う。このとき、コンテンツが正規に光ディスク1101に記録されている場合は、光ディスク1101に記録されている暗号化コンテンツを復号するための鍵は光ディスク1101のディスクIDであり、BCA再生回路1521から出力されるディスクID信号も、光ディスク1101のディスクID信号（BCAS）であるので、第2暗号デコーダ1520は正常に復号処理を実行することができる。従って、復号又はデスクランブルされたコンテンツのデータは第2暗号デコーダ1520から出力信号1525として出力される。ここで、第2暗号デコーダ1520の復号化処理は次式で表記することができ、コンテンツが画像信号の場合は、第2暗号デコーダ1520は、例えばMPEG信号を伸長して元の画像信号を再生して出力する。

【0152】

【数7】 $C[BCAS] \# BCAS = C$

【0153】また、上記光ディスク1101はディスクID信号（BCAS）1515のみで暗号化されているので、BCA再生回路1521と第2暗号デコーダ1520を有する任意の光ディスク記録再生装置で再生することが可能である。なお、暗号エンコーダ1504、1516で暗号化し、暗号デコーダ1513、1520で復号化することを説明したが、各装置1501、1506、1514内の制御部であるCPUで実行されるプログラムに、暗号アルゴリズム及び復号アルゴリズムのプ

ログラムを備えて暗号化や復号化を実行するように構成してもよい。

【0154】なお、本実施形態において、CATVデコーダ1506の第2暗号化エンコーダ1516はディスクID信号1515を第2暗号鍵として用いてコンテンツを暗号化したか、以下のようにコンテンツを暗号化してもよい。例えば各CATV会社装置1501毎に準備されたICカード1522をCATVデコーダ1506に装着して、ICカード1522の会社識別信号メモリ1523内に記録されている会社識別信号と、BCA再生回路1521により再生されたディスクID信号（BCAS）を組み合わせて第2暗号鍵として用いて、第2暗号化エンコーダ1516によりコンテンツを暗号化してもよい。ここで、第1暗号デコーダ1513の出力信号であるコンテンツをCとし、第1の第2暗号鍵であるディスクID信号1515をBCASとし、第2の第2暗号鍵である会社識別信号1523をCKとし、第2暗号化コンテンツ1517をC[BCAS, CK]とすると、第2暗号化エンコーダ1516の暗号化処理を次式のように表記される。

【0155】

【数8】 $C * BCAS * CK = C[BCAS, CK]$

【0156】次に、光ディスク1101に暗号化して記録されたコンテンツを再生する際には、光ピックアップから出力されるレーザ光が光ディスク1101の上記暗号化されたコンテンツが記録されている領域を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射される反射光を再生信号に光電変換してデータ再生部1519に出力する。データ再生部1519は入力される再生信号をデジタル再生信号にA/D変換して第2暗号デコーダ1520に出力する。一方、光ピックアップから出力されるレーザ光は光ディスク1101のBCA1104を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射される反射光を再生信号に光電変換してBCA再生回路1521に出力する。BCA再生回路1521は入力される再生信号に基づいてディスクID信号1515を再生して、ディスクID信号1515を第2暗号化エンコーダ1516及び第2暗号デコーダ1520に出力する。

【0157】さらに、光ディスク記録再生装置1514に装着されたICカード1524の会社識別信号メモリ1526内の会社識別信号は、第2暗号デコーダ1520に入力される。なお、当該会社識別信号は、ICカード1524の会社識別信号メモリ1526内に記録されていなくてもよく、例えば、光ディスク記録再生装置1514の記録プログラムのインストール時に、会社識別信号が、光ディスク記録再生装置1514の制御部であるCPUに接続されたメモリ（図示せず。）に記録されていてもよい。とって代わって、会社識別信号を光ディスク記録再生装置1514のキーボード（図示せず。）

を用いて入力してもよい。

【0158】第2暗号デコーダ1520は、入力されたディスクID信号1515と、会社識別信号を復号鍵として用いて、暗号化されたコンテンツの復号を行う。このとき、CATVデコーダ1506のユーザがCATV会社装置1502を有する特定のCATV会社と正式に契約をし、コンテンツ1502が正規に光ディスク1101に記録されている場合は、光ディスク1101に暗号化されて記録されている暗号化コンテンツの第1の復号鍵は、まさに再生しようとする光ディスク1101のディスクID信号(BCAS)であり、第2の復号鍵は、契約したCATV会社から提供されたICカード1524の会社識別信号メモリ1526内の会社識別信号(CK)である。従って、復号又はデスクランブルされたコンテンツの出力信号1525が、第2暗号デコーダ1520から出力される。ここで、第2暗号デコーダ1520の復号化処理は次式のように表記され、コンテンツが画像信号の場合は、例えばMPEG信号が第2暗号デコーダ1520により伸長されて、画像信号の出力信号1526が出力される。

【0159】

【数9】

$C[BCAS, CK] \# (BCAS * CK) = C$

【0160】また、上記光ディスク1101のコンテンツは、ディスクID信号1515と会社識別信号で暗号化されているので、上記コンテンツの提供元のCATV会社と契約を結んでいれば、BCA再生回路1521と、第2暗号デコーダ1520を有する任意の光ディスク記録再生装置で再生することが可能である。逆に、上記CATV会社と契約していなければ、会社識別信号を入力できないので、コンテンツを再生することができず、契約済みのユーザとの差別化を可能にする。

【0161】また、本実施形態では、各ユーザは自宅のCATVデコーダ1506に光ディスク記録再生装置1514からディスクID信号を送り、画像データ等を暗号化するので、CATV会社装置1501は各ユーザに配信する暗号化コンテンツを個別に渡える必要がなく、放送時のシステムを簡単にでき、低コストで、大量の視聴者に同じコンテンツを提供することができる。さらに、本実施形態によれば、CATVデコーダ1506を有する各ユーザ毎にRAM型光ディスク1枚だけに記録を許可することができる。

【0162】なお、本実施形態では、ケーブルテレビジョンのヘッドエンドからコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【0163】<第5の実施形態>さらに、本発明に係る第5の実施形態である暗号化コンテンツ記録及び再生方法について図面を参照しながら説明する。図21は、本発明に係る第5の実施形態である光ディスク1601のデータ記録領域を示す平面図であり、図22は、第5の

実施形態に係る光ディスク記録再生システムの構成を示すブロック図である。なお、第5の実施形態において、第3及び第4の実施形態と共通の部分はその説明を簡略化する。

【0164】図21において、1601は書き換え型又は追記型光ディスクである記録型光ディスク、1602はディスク情報を凹凸ビットの形式で記録されたコントロールユーザデータ領域、1603はレーザ光の光ビームを光ディスクに照射することによりユーザがデータを記録するためのユーザデータ領域、1604はディスクIDが記録されたBCAである。

【0165】BCA1604では、コントロールユーザデータ領域1602の内周部分の凹凸ビット上の記録膜が部分的にYAGレーザなどのパルスレーザでトリミングされることにより、半径方向に長い形状でかつ複数のトリミング領域1606が形成される。なお、トリミングはディスク製造者によって行われる。また、BCA1604に記録されるデータにディスクIDを付加することにより、光ディスクの管理を容易に実現することができる。さらに、BCA1604のデータが凹凸ビット上に記録されることにより、BCA1604に記録された、光ディスクを識別する情報が容易に改ざんされることを防止することができる。

【0166】さらに、コントロールユーザデータ領域1602とBCA1604が隣接していることにより、コントロールユーザデータ領域1602のデータを再生する際に、BCA1604のデータも続けて再生することができ、もしくはBCA1604のデータを再生する際に、コントロールユーザデータ領域1602のデータを続けて再生することができるので、例えば光ディスクを起動する際にCPUが速やかにディスクを識別するためのBCA1604の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【0167】なお、本実施形態のBCA1604を、コントロールユーザデータ領域1602の内周部分の凹凸ビット上の記録膜をトリミングすることにより形成しているが、書き換え型又は追記型光ディスクである記録型光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールユーザデータ領域1602の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からユーザデータ領域1603の記録データを保護することができる。また、コントロールユーザデータ領域1602の内周側にBCA1604を形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する場合のマージンを考慮しているためである。なお、トリミング前のBCA1604に記録されているデータが、コントロールユーザデータ領域1602に記録されていてよい。BCA1604に記録されているデ

ータが、コントロールユーザデータ領域1602にも記録されていることにより、トリミングを行ってもコントロールユーザデータ領域1602の上記データを保護することができる。

【0168】さらに、上記データが、BCA1604から、コントロールユーザデータ領域1602まで連続して繰り返し記録されている場合には、コントロールユーザデータ領域1602の上記データを見つけることによって、BCA1604の位置を予想することができる。また、鍵情報記録領域1606のデータは、ユーザデータ領域1603と同じく光ビームを照射することにより記録される。

【0169】本実施形態のように、コントロールユーザデータ領域1602と鍵情報記録領域1606が隣接していることにより、コントロールユーザデータ領域1602のデータを再生する際に、鍵情報記録領域1606のデータも続けて再生することができ、もしくは鍵情報記録領域1606のデータを再生する際に、コントロールユーザデータ領域1602のデータを続けて再生することができるので、例えば光ディスクを起動する際にCPUが速やかにディスクを識別するためのBCA1604の情報を入手し、暗号化されたコンテンツを再生するための処理を早めることが可能になる。

【0170】図22において、第5の実施形態に係る光ディスク記録再生システムは、CATV会社装置1701と、鍵発行センター装置1707と、CATVデコーダ1706と、光ディスク記録再生装置1714と、テレビジョン装置1730とを備えて構成される。ここで、CATV会社装置1701は、映画ソフトウェアなどのコンテンツを格納するコンテンツメモリ1702と、第1暗号鍵を格納する第1暗号鍵メモリ1703と、第1暗号化エンコーダ1704とを備える。また、CATVデコーダ1706はシステムIDメモリ1708と、第1暗号デコーダ1713と、現在時刻情報を出力するクロック回路1725とを備える。さらに、鍵発行センター装置1707は、当該装置1707の動作を制御する制御部1707aと、時間制限情報を格納する時間制限情報メモリ1710とを備える。またさらに、光ディスク記録再生装置1714は、記録回路1717と、鍵情報記録回路1719と、BCA再生回路1720と、データ再生部1721と、第2暗号デコーダ1722と、鍵情報再生部1723とを備える。

【0171】まず、CATV会社装置1701の第1暗号化エンコーダ1704は、コンテンツメモリ1702内の映画ソフトウェアなどのコンテンツのデータを第1暗号鍵1703を用いて暗号化することにより、第1暗号化コンテンツ1705を生成し、ネットワークを介して各ユーザのCATVデコーダ1706の第1暗号デコーダ1713に送信する。ここで、コンテンツメモリ1702内のコンテンツをCとし、第1暗号鍵メモリ17

03内の第1暗号鍵をFKとし、第1暗号化コンテンツ1705をC[FK]とすると、次式のように表記される。

【0172】

【数10】 $C * FK = C[FK]$

【0173】CATVデコーダ1706は、CATVデコーダ1706のシステムIDメモリ1708内のシステムIDと、例えばキーボード（図示せず。）を用いて入力された、視聴したい上記コンテンツのタイトルコード1709を、ネットワークを介して鍵発行センター装置1707の制御部1707aに送信する。なお、上記タイトルコードは、テレビジョン装置1730の画面に従って選択することにより入力してもよいし、直接キーボードから入力してもよいし、リモートコントローラ等から入力してもよい。従って、タイトルコードは、ユーザが独自に入手していてもよいし、第1暗号化コンテンツとともにCATVデコーダ1706に送られてきてもよいし、番組案内などの形態で第1暗号化コンテンツとは別の時刻に予め送られていてもよい。

【0174】鍵発行センター装置1707の制御部1707aは、CATVデコーダ1706のシステムIDと、上記コンテンツのタイトルコードとに基づいて、時間制限情報メモリ1710内の対応する時間制限情報を参照して、対応する鍵(K)1712を生成して、CATVデコーダ1706の第1暗号デコーダ1713にネットワークを介して送信する。なお、時間制限情報により、同一のコンテンツを時刻を変えて複数回放送する場合を区別することができる。ここで、第1復号鍵をFKとし、CATVデコーダ1706のシステムIDをDIDとし、時間制限情報をTIMEとし、コンテンツのタイトルコードをTとすると、鍵(K)1712は、次式の関係を満たしている。

【0175】

【数11】 $FK = K * T * DID * TIME$

【0176】第1暗号デコーダ1713は、第1復号鍵(FK)と、鍵発行センター装置1707から送信されてくる上記鍵(K)1712と、上記コンテンツのタイトルコードと、システムIDと、時間制限情報とが上述の関係を満たしており、かつ時間制限情報がクロック回路1725からの現在時刻情報の条件を満たしていれば、第1暗号化コンテンツ1705を復号することができる。ここで、第1暗号化コンテンツ1705が画像信号の場合は、デスクランブルされた画像信号が第1暗号化デコーダ1713からテレビジョン装置1730に出力され、ユーザはコンテンツをテレビジョン装置1730で視聴できる。ここで、第1暗号化デコーダ1713の復号処理は次式のように表記される。

【0177】

【数12】

$C[FK] \# (K * T * DID * TIME)$

$=C[FK] \# FK$
 $=C$

【0178】次に、上記コンテンツを光ディスク1601に記録する方法を説明する。光ディスク1601にコンテンツを記録する際には、CATVデコーダ1706にて復号化されていない、第1暗号化コンテンツ1705が、CATV会社装置1701の第1暗号化エンコーダ1704から光ディスク記録再生装置1714の記録回路1717に送信される。記録回路1717は、受信された第1暗号化コンテンツ1705のデータを、例えば公知の8/16変調方式などの変調方式を用いてデジタル変調し、変調後のデジタルデータは、光ピックアップ（図示せず。）により光ディスク1601に記録される。従って、光ディスク1601に暗号化されて記録された上記コンテンツを再生するためには、第1暗号化コンテンツ1705を復号する必要がある。

【0179】光ディスク記録再生装置1714は、BCA再生回路1720により再生された、光ディスク1601のディスクID信号1715と、例えばキーボード（図示せず。）を用いて入力された、再生したい上記コンテンツのタイトルコード1716とを、ネットワークを介して鍵発行センター装置1707の制御部1707aに送信する。なお、ディスクIDを送るタイミングは、鍵発行センター装置1707とアクセスする際に送ってもよいし、もしくは、視聴の際に、タイトルコードと一緒に送ってもよい。

【0180】また、ディスクIDの送信方法として、図22に示すように光ディスク1601のBCA1604を再生して、BCA再生回路1720の出力信号を直接鍵発行センター装置1707に送る方法を上記で開示しているが、本発明はこれに限らず、下記の方法を用いてもよい。例えばディスク起動時などの、鍵発行センター装置1707とのアクセス以前に、BCA1604のデータを再生して、光ディスク記録再生装置1714又はCATVデコーダ1706のメモリ（図示せず。）に保管しておき上記タイミングで鍵発行センター装置1707の制御部1707aに送信してもよい。さらに、ディスクIDが、ラベルなどの形態で視覚的にも認識できる場合には、キーボードから入力してもよいし、ラベルがバーコードになっている場合にはバーコードリーダーから読みとってよい。

【0181】鍵発行センター装置1707の制御部1707aは、光ディスク1601のディスクID信号1715及びコンテンツのタイトルコード1716に対応する鍵（DK）1718を生成して、光ディスク記録再生装置1714の鍵情報記録回路1719に送信する。ここで、第1復号鍵をFKとし、光ディスク1601のディスクID信号1715をBCASとし、コンテンツのタイトルコード1716をTとすると、鍵（DK）は、次式の関係を満たしている。

【0182】

【数13】 $FK = DK * BCA * T$

【0183】光ディスク記録再生装置1714の鍵情報記録回路1719に入力された鍵（DK）は、例えば公知の8/16変調方式などの変調方式を用いてデジタル変調され、変調後のデジタルデータが光ピックアップ（図示せず。）により光ディスク1601の鍵情報記録領域1605に記録される。なお、鍵（DK）は鍵情報記録領域1605に、同一の鍵が複数個記録されてもよい。同一の鍵が複数個記録されることにより、鍵情報記録領域1605の記録膜が劣化した場合や、光ディスク1601に傷がついた場合に鍵（DK）を保護することができ、いずれか1つの鍵（DK）のデータを再生することができれば、コンテンツを復号できる。

【0184】また、本実施形態では、鍵情報記録領域1605はユーザデータ領域1603の内周側に設けられているが、ユーザデータ領域1603の外周側にあってもよく、内周側と外周側の両方に設けられていてもよい。外周側に設けられることにより、より多くの鍵（DK）を記録することが可能となる。また、鍵情報記録領域が複数個、分散して設けられることにより、1つの鍵情報記録領域が再生できなくなった場合でも、他の鍵情報記録領域により鍵（DK）を保護することができる。

【0185】一方、光ピックアップから出力されるレーザ光が光ディスク1601の上記コンテンツが記録された領域を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をデータ再生部1721に出力する。これにตอบสนองして、データ再生部1721は、入力された再生信号を暗号化デジタルデータにA/D変換して第2暗号デコーダ1722に出力する。さらに、光ピックアップから出力されるレーザ光は光ディスク1601のBCA1604を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をBCA再生回路1720に出力する。これにตอบสนองして、BCA再生回路1720は、入力される再生信号に基づいてディスクID信号1715を再生して、暗号デコーダ1722に出力する。さらに、光ピックアップから出力されるレーザ光は光ディスク1601の鍵情報記録領域1605を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換して再生信号を鍵情報再生部1723に出力し、これにตอบสนองして、鍵情報再生部1723は、入力される再生信号に基づいて鍵（DK）のデータを生成して、第2暗号デコーダ1722に出力する。

【0186】なお、鍵発行センター装置1707に対してアクセスしてすぐにコンテンツを再生する際は、鍵情報記録回路1719は、鍵（DK）を鍵情報記録領域1605に記録する前に、直接に第2暗号デコーダ172

2に入力してもよい。このようにすることにより、再生を開始するまでの時間を短縮することができる。暗号デコーダ1722は、入力されたディスクID信号1715と、鍵(DK)と、上記コンテンツのタイトルコード1716とからなる復号鍵を用いて、暗号化されたコンテンツの復号を行う。第2暗号デコーダ1722の復号化処理は次式で表される。コンテンツが画像信号の場合は、例えばMPEG信号が伸長されて、画像信号の出力信号1724が第2暗号デコーダ1722から出力される。

【0187】

【数14】

$C[FK] \# (DK * BCA * T)$

$= C[FK] \# FK$

$= C$

【0188】本実施形態において、鍵発行センター装置1707の制御部1707aから鍵信号を受信するときに課金されるとすると、視聴するときに、光ディスク1601に記録したコンテンツを初めて再生するときに別々に課金され、光ディスク1601に記録しただけでは課金されない。従って、視聴と光ディスク1601への記録の両方に対してまとめて課金する場合に対して、視聴はしたいが光ディスク1601に記録する必要がないユーザや、光ディスク1601に記録したいが、放送されるときに視聴する必要がないユーザにとっては課金される金額を安くすることができる。また、光ディスク1601に記録しただけでは課金されないで、ユーザは視聴した後で、再度視聴するために光ディスク1601を再生するための鍵を受け取るかどうかを決定することができる。以上の実施形態においては、鍵(DK)は鍵発行センター装置1707の制御部1707aからネットワークを介して受信する方法を用いているが、本発明はこれに限らず、コンテンツのタイトルとディスクID番号を電話等で口頭で伝えることにより、口頭で受け取ってキーボードから入力してもよい。

【0189】次に、鍵情報記録領域1605に鍵(DK)が記録された光ディスク1601を鍵発行センター装置1707とのアクセス終了後に再生する場合について説明する。まず、光ピックアップから出力されるレーザー光が光ディスク1601の上記コンテンツが記録された領域を照射し、その反射光が光電変換を行う光ピックアップを介してデータ再生部1721に入力される。これにตอบสนองして、データ再生部1721は暗号化されたコンテンツのデータを第2暗号デコーダ1722に出力する。一方、光ピックアップから出力されるレーザー光は光ディスク1601のBCA1604を照射し、その反射光が光電変換を行う光ピックアップを介してBCA再生回路1720に入力される。これにตอบสนองして、BCA再生回路1720は入力される再生信号に基づいてディスクID信号1715を生成して第2暗号デコーダ1722

2に出力する。

【0190】さらに、光ピックアップから出力されるレーザー光は光ディスク1601の鍵情報記録領域1605を照射し、その反射光が光電変換を行う光ピックアップを介して鍵情報再生部1723に入力される。これにตอบสนองして、鍵情報再生部1723は入力される再生信号に基づいて鍵(DK)のデータを生成して第2暗号デコーダ1722に出力する。第2暗号デコーダ1722は、入力されたディスクID信号1715と、鍵(DK)と、上記コンテンツのタイトルコード1716からなる復号鍵を用いて、データ再生部1721から出力される、暗号化されたコンテンツの復号を行う。第2暗号デコーダ1722の復号化処理は次式で表される。コンテンツが画像信号の場合は、例えばMPEG信号が伸長されて、画像信号が第2暗号デコーダ1722から出力される。

【0191】

【数15】

$C[FK] \# (DK * BCA * T)$

$= C[FK] \# FK$

$= C$

【0192】鍵情報記録領域1605に鍵(DK)のデータが一度記録されることにより、鍵発行センター装置1707とのアクセスをすることなく、常に上記暗号化コンテンツを再生することができる。また、復号化処理に必要な復号鍵は全て光ディスク1601に記録されているので、上記光ディスク1601は、BCA再生回路1720と、鍵情報再生部1723と、第2暗号デコーダ1722とを有する任意の光ディスク記録再生装置で再生することができる。

【0193】さらに、上記暗号化コンテンツをディスクIDの異なる光ディスク1601にコピーして再生しようとした場合には、BCA再生回路1720から上記光ディスク1601とは異なるディスクID信号が出力されるので、暗号化されたコンテンツを復号することができず、コンテンツはコピーされても再生されない。ただ、この場合にも、コンテンツのタイトルとディスクIDをネットワークもしくは口頭で鍵発行センターに伝えることにより、課金の後、復号鍵を受け取ってもよい。このように、暗号化されたコンテンツを別の光ディスク1601にコピーされても、不正に再生されることはなく、暗号化されたコンテンツをコピーした光ディスク1601を再生する際には必ず課金が伴うことから著作権を保護することができる。

【0194】図23は、第5の実施形態に係るID付与テーブルの構成を示す表であり、システムIDやディスクIDが異なる場合の第1暗号デコーダ1713に入力される鍵(K)と、鍵情報記録回路1719に入力される鍵(DK)とを整理して示したものである。図23において、T1、T2、T3は異なるコンテンツのタイト

ルコードであり、FK1、FK2、FK3はそれぞれT1、T2、T3のタイトルコードを有する暗号化コンテンツを復号するための復号鍵である。また、DID1、DID2、DID3はそれぞれ異なるCATVデコーダ1706のシステムIDであり、BCAS1、BCAS2、BCAS3はそれぞれ異なる光ディスク1601のディスクIDである。このとき、CATVデコーダ1706に入力される鍵(Kmn)は、次式を満足するように決定される。

【0195】

【数16】 $FK_n = K_{mn} * T_n * DID * TIME_n$

【0196】また、光ディスク記録再生装置1714に入力される鍵(DKmn)は、次式を満足するように決定される。

【0197】

【数17】 $FK_n = DK_{mn} * BCAM * T_n$

【0198】図23に示すように、コンテンツが異なるときはもちろんのこと、コンテンツが同じ場合でも、異なるCATVデコーダ1706、異なる光ディスク、異なる放送時間毎に鍵発行センター装置1707から入手する鍵情報は異なることから細部にわたる著作権の保護が可能になる。同様に、コンテンツが同じでもシステムID、ディスクID、時間情報が異なれば鍵情報が異なることから、CATV会社装置1701は、ユーザ毎に暗号化コンテンツを変える必要がなく、1つのコンテンツに対して1つの暗号化コンテンツを準備すればよい。これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【0199】なお、本実施形態では、ケーブルテレビジョンのヘッドエンドからのコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【0200】<第3乃至第6の実施形態の効果>本実施形態に係る光ディスクは、第1のディスク情報が記録されている第1の情報領域と、個々のディスクを識別するための第2のディスク情報が記録されている第2の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する。従って、従来技術の光ディスクに、上記光ディスクを識別する情報を付加することにより、光ディスクの管理を容易に実現することができる。ここで、上記第2の情報領域は、好ましくは、上記第1の情報領域内に記録されているものであり、上記第1の情報領域を再生する光ピックアップによって再生することができる。また、上記第2の情報領域は、上記第1の情報領域内の記録膜を、半径方向に長い形状でかつ複数個のトリミング領域が形成されるように、部分的に除去することにより記録されているものであり、容易に上記第2のディスク情報が改ざんされることを防止することができる。

【0201】また、本実施形態に係る暗号化コンテンツの記録方法によれば、第1のディスク情報が記録されて

いる第1の情報領域と、個々のディスクを識別するための第2のディスク情報が記録されている第2の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する光ディスクの上記ユーザデータ領域にコンテンツのデータを記録する際に、少なくとも上記第2のディスク情報を用いた演算によりコンテンツのデータを復号して再生することができるように、コンテンツのデータを暗号化して記録する。従って、特定の1枚の光ディスクにしか存在しない光ディスクの識別情報を用いて、コンテンツを暗号化することにより、コンテンツの不正なコピーを防止することができ、著作権が保護できるという特有の効果がある。

【0202】さらに、本実施形態に係る光ディスクは、ユーザデータ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する。従って、暗号化されて記録されたコンテンツを解読する際に鍵情報が必要なシステムにおいて、鍵情報記録領域に鍵情報が一度記録されることにより、再生する度に鍵情報を入力する必要がなくなるという特有の効果がある。

【0203】またさらに、本実施形態に係る暗号化コンテンツの記録方法によれば、第1のディスク情報が記録されている第1の情報領域と、個々のディスクを識別するための第2のディスク情報が記録されている第2の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域と、ユーザデータ領域内に、暗号化されて記録されたコンテンツのデータを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの上記ユーザデータ領域にコンテンツを記録する際に、少なくとも上記第2のディスク情報と、上記鍵情報を用いた演算によりコンテンツのデータを復号して再生することができるようにコンテンツのデータを暗号化して記録する。従って、暗号化されたコンテンツのデータを別の光ディスクにコピーされても、不正に再生されることはなく、暗号化されたコンテンツのデータをコピーした光ディスクを再生する際には必ず課金に伴うことから著作権を保護することができる。

【0204】ここで、第1のディスク情報は、好ましくは、微少な凹凸ビットにより構成され、光ディスクを識別するための第2のディスク情報が、上記凹凸ビット上に記録される。従って、容易に第2のディスク情報が改ざんされることを防止することができる。さらに、好ましくは、上記第1のディスク情報と第2のディスク情報が隣接するように形成される。これにより、上記第1のディスク情報を再生する際に、第2のディスク情報も続けて再生することができ、もしくは第2のディスク情報を再生する際に、第1のディスク情報を続けて再生することができるので、例えば光ディスクを起動する際にCPUが速やかにディスクを識別するための第2のディスク情報を入手し、暗号化されたコンテンツを記録するた

めの処理を早めることが可能になる。

【0205】また、本実施形態に係る暗号化データの記録方法によれば、コンテンツが同じでもシステムID、ディスクID、時間情報が異なれば鑑情報異なることから、CATV会社装置701は、ユーザ毎に暗号化コンテンツを変える必要がなく、1つのコンテンツに対して1つの暗号化コンテンツを準備すればよく、これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【0206】<第3及び第5の実施形態の変形例>以上の第3と第5の実施形態においては、図16及び図21に示すように、トリミング領域1105、1606はそれぞれ、コントロールユーザデータ領域1102、1602内の内周部に位置するBCA1104、1604に形成しているが、本発明はこれに限らず、それぞれ第3と第5の実施形態の変形例に係る光ディスク1101a、1601aのデータ記録領域を示す図24及び図25に示すように、コントロールユーザデータ領域1102、1602から光ディスクの内周側にはみ出るように記録誤をトリミングしてトリミング領域1105a、1606aを形成してもよい。すなわち、BCA1104a、1604aはそれぞれ、コントロールユーザデータ領域1102、1602内に含まれず、コントロールユーザデータ領域1102、1602の内周部から、コントロールユーザデータ領域1102、1602の内側にはみ出るように配置されて形成される。この変形例において、BCA1104a、1604aをこのように形成するのは、フォーカスサーボ回路の不安定性によりレーザー光のビームのスポットの径が変化する場合のマージンを考慮しているためである。この変形例においても、コントロールユーザデータ領域1102、1602の外側にユーザデータ領域1103、1603が存在しているので、これらのユーザデータ領域1103、1602に記録されたデータを破壊しないように保護するために、トリミング領域1105a、1606aが配置されて形成される。

【0207】<第6の実施形態>図26は、本発明に係る第6の実施形態である光ディスク内のユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。本実施形態において、光ディスクは、例えば、DVD-RAMなどの記録型光ディスクである。

【0208】図26に示すように、ユーザデータ領域2150は、セクタヘッダ領域2101と、メインデータ領域2102と、誤り検出コード2103とから構成される。セクタヘッダ領域2101には、セクタの位置を示すセクタアドレス2104と、メインデータ領域2102に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報などを含む。）が記録される著作権制御情報2105とが記録されるとともに

に、セクタヘッダ領域2101は、メインデータ領域2102のデータに暗号が施されている場合に復号するための復号鍵領域2106を含む。また、メインデータ領域2102は、非暗号化コンテンツ2107が記録される領域と、暗号化コンテンツ2108が記録される領域とに分割され、非暗号化コンテンツ2107は、MPEGにおける同期パターンや、各種制御情報などの後続するデータの制御情報を含む。さらに、暗号化コンテンツ2108は、主に著作権保護を必要とするAVデータなどが暗号化されたコンテンツのデータを含む。

【0209】復号鍵領域2106には、後続するメインデータ領域2102を再生するための復号鍵が所定のサイズを有する複数の分割された復号鍵（以下、分割復号鍵という。）に分割されて記録される。例えば、4バイトの1つの復号鍵領域に対して復号鍵が8バイトである場合、8バイトの復号鍵を各4バイトの分割復号鍵に分割し、論理的に連続する2つのセクタの復号鍵領域2106、2109にそれぞれ、分割された2つの分割復号鍵を記録する。このようなユーザデータ領域の再生時には、論理的に連続する（ただし、欠陥等により使用不可能なセクタはスキップする。）複数のセクタの復号鍵領域2106、2109から分割された複数の分割復号鍵を取得し、取得された必要数の分割復号鍵をデータ連結器2111にて連結し、再生に必要な暗号化復号鍵（8バイト）を得る。暗号化復号鍵（8バイト）を得ることのできたセクタのメインデータ領域2102に記録されたデータに対して、それぞれの著作権制御情報2105の内容に従って、復号器2114を用いて復号化処理を実行する。

【0210】さらに、より暗号の強度を高めるために、復号鍵に対して暗号化を施すことも可能であるし、暗号の結果が一定とならないように、データ中の情報である復号鍵変換データを鍵に加えることにより、同一の暗号鍵であっても、異なる暗号結果を提供することも可能である。具体的には、図26に示すように、データ連結器2111から出力される暗号化復号鍵が鍵復号器2112に入力され、鍵復号器2112は、入力された暗号化復号鍵を、所定のディスク鍵を用いて、ダミーデータであるパディングデータ（1バイト）と復号鍵（7バイト）に復号化して鍵変換器2113に出力する。ここで、ディスク鍵は、例えば、光ディスクに記録された暗号化ディスク鍵を、所定のマスター鍵である秘密鍵を用いて、ディスク鍵復号器（図示せず。）により復号することにより取得される。次いで、鍵変換器2113は、メインデータ領域2102から読み出した復号鍵変換データ2110を、上記鍵復号器2112から出力される復号鍵を用いて、例えば乗算や除算、所定の重み係数を用いた演算などの所定の変換演算によりデータ変換することによりコンテンツ復号鍵（7バイト）を生成して復号器2114に出力する。そして、復号器2114は、

メインデータ領域2102から読み出したコンテンツのデータを、上記鍵変換器2113から出力されるコンテンツ復号鍵(7バイト)を用いて復号することにより、復号化されたコンテンツのデータを生成して出力する。なお、復号鍵変換データ2110としては、コピー世代管理情報や、アナログのマクロビジョン制御フラグなどの改ざんがされることによりデータの不正利用がすぐに検出可能であるようなデータを利用することが好ましい。

【0211】図27は、第6の実施形態に係る光ディスクにおいて、ユーザデータ領域への著作権制御情報と復号鍵の配置と、メインデータ領域への暗号化コンテンツの配置を示すブロック図である。図27に図示されたユーザデータ領域2160の一例においては、復号鍵領域2201と、4バイトの分割復号鍵を有する第1の復号鍵領域2202と、4バイトの分割復号鍵を有する第2の復号鍵領域2202とに分割されて配置されている。このため、これらの2つのセクタに記録する暗号化コンテンツの大きさに応ず、複数のセクタ(図27では2つのセクタ)が使用されることとなる。この場合、未使用の領域には、ダミーデータが補完データとして記録される。図27の例では、1セクタ分の暗号化コンテンツ2204しかない場合には、1セクタ分の補完データ2203が記録される。

【0212】図28は、第6の実施形態に係る光ディスクにおいて、エラー訂正の単位が複数のセクタにまたがる場合の配置を示すブロック図である。例えば、光ディスクがDVDである場合、16セクタのエラー訂正コードの単位ブロック(以下、ECCブロックという。)を用いることにより、エラー訂正の能力を高めている。このため、データの記録や再生を行う際には、ECCブロック単位での記録が必要となる。復号鍵を任意の複数の分割復号鍵に分割して記録を行ったとすると、1つの復号鍵が複数のエラー訂正ブロックにまたがって記録される場合が発生する。再生の際には、分割された複数の分割復号鍵のすべてを再生する必要があるため、暗号化コンテンツのデータを記録したセクタ以外にも、復号鍵を記録した直前のECCブロックまでも再生する必要がある。図28の例では、復号鍵を分割するときの分割数をECCブロックのセクタ数の約数に設定することの特徴としている。これにより、分割された複数の分割復号鍵がECCブロックにまたがって記録されることがなくなる。さらに、1つのECCブロック内で使用する復号鍵として、1種類の復号鍵のみを用い、記録するAVデータがECCブロックに満たない場合には、補完データ、並びに補完セクタを配置することによって、再生時に不要なセクタのデータを光ディスクから読み出すことを防止することができる。

【0213】<第7の実施形態>図29は、本発明に係る第7の実施形態である光ディスク内のリードイン領域

2401とユーザデータ領域2402の構成と、リードイン領域2401とユーザデータ領域2402のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。

【0214】図29において、図26の第6の実施形態と同様に、リードイン領域2401とユーザデータ領域2402はそれぞれ、セクタヘッダ領域2101と、メインデータ領域2102と、誤り検出コード2103とを有するセクタから構成される。セクタヘッダ領域2101には、セクタの位置を示すセクタアドレス2104と、メインデータ領域2102に記録されるデータに関する著作権制御情報(スクランブルフラグ、コピー制御情報などを含む。)が記録される著作権制御情報2105とが記録されるとともに、セクタヘッダ領域2101は、メインデータ領域2102のデータに対して暗号が施されている場合に復号するための復号鍵を参照するための、復号鍵の記録位置(メインデータ領域2102内の復号鍵テーブル2404での記録位置又は格納位置をいう。)を示す鍵インデックスを記録する鍵インデックス領域2403を含む。ユーザデータ領域2402に記録された暗号化コンテンツを復号するための復号鍵は、テーブル形式で書き換え可能なリードイン領域2401に復号鍵テーブル2404の形式で記録される。鍵インデックス領域2403に記録される鍵インデックスによりリードイン領域2401に記録された復号鍵が参照される。図26に図示された第6の実施形態と同様に、上記参照された復号鍵は、所定のディスク鍵を用いる鍵復号器2112によりパディングデータと復号鍵(又はタイトル鍵)とに復号された後、上記復号された復号鍵(又はタイトル鍵)は、復号鍵変換データを用いる鍵変換器2113によりコンテンツ復号鍵に変換されて復号器2114に出力される。復号器2114は、暗号化されたコンテンツのデータを、コンテンツ復号鍵を用いて復号することにより、復号化コンテンツのデータを生成して出力する。

【0215】以上のように構成された第7の実施形態に係る光ディスクと光ディスク再生装置においては、セクタヘッダ領域2101内にある鍵インデックス領域2403に参照用の鍵インデックスを記録することにより、鍵インデックス領域2403のサイズとは独立に復号鍵テーブル2404の復号鍵サイズを割り当てることができる。また、復号鍵テーブル2404のサイズを割り当てた後も、鍵インデックス領域2403内の鍵インデックスで示される復号鍵テーブル2404から連続して複数の復号鍵を使用することにより、自由なサイズの復号鍵を利用することができる。

【0216】図30(a)は第7の実施形態に係る光ディスク内のリードイン領域2401のメインデータ領域2102において、復号鍵の初期値で未記録状態を表示する場合のデータ構成を示すブロック図である。図30

(a)において、光ディスクのフォーマット時などにおいて記録される復号鍵の初期値として、鍵として使用しない既知の固定値（例えば、オール0などのデータ）である未記録状態データ2501を記録し、これにより、復号鍵の未記録状態を示す。

【0217】図30(b)は第7の実施形態に係る光ディスク内のリードイン領域2401のメインデータ領域2102において、復号鍵状態テーブルで記録状態を表示する場合のデータ構成を示すブロック図である。図30(b)においては、図30(a)に図示された復号鍵と同様に、インデックスにより参照可能なテーブル形式の復号鍵状態テーブル2502をリードイン領域2401に配置し、復号鍵の記録状態を記録状態データ2503として以下のように記載している。

- (1) 0×00：未使用、
- (2) 0×01：領域予約、
- (3) 0×03：鍵記録済み、
- (4) その他：予約済み。

ここで、0×は、それに続く文字について16進数表示を示す。

【0218】図31は、第7の実施形態に係る光ディスクにおいて復号鍵の配置を示すブロック図である。図31の例では、復号鍵の信頼性を高めるためにディスク上への復号鍵領域の配置を工夫している。通常、ユーザデータ領域2602においては欠陥管理が行われるため、書き込み不良が発生した場合には、代替領域等へ交代処理が行われる。しかしながら、リードイン領域2601では、上記のような欠陥管理は行われない。このため、書き込み不良や読み出し不良などの発生により、AVデータの再生に必要な復号鍵が利用不能となり、さらには光ディスクそのものが利用不能となる場合がある。従って、異なる複数のECCブロックにわたって、合計複数の復号鍵を記録しておくことが望ましい。また、近接した領域に複数の復号鍵を記録した場合、傷や埃等により複数記録したものがすべて読めなくなる場合がある。このため、図31に示すように、リードイン領域2601とリードアウト領域2603においてそれぞれ、光ディスクの内周側と外周側といったようなレイアウト上離れた位置に各復号鍵を記録しておくことがより好ましい。

【0219】なお、図29の実施形態においては、復号鍵領域をリードイン領域2401、2601に配置している。これは、ユーザデータ領域2602が通常のリードコマンドやライトコマンドでアクセス可能な領域であることを考慮し、パーソナルコンピュータのドライブ装置などからアクセスするときの安全性を高めるためである。従って、これらをユーザデータ領域2602に配置しても、同様の効果を得ることができる。

【0220】＜第8の実施形態＞図32は、本発明に係る第8の実施形態である光ディスクのデータをファイル管理システムにより管理するときのデータ構成を示すブ

ロック図である。図32の例では、ファイルシステムの構造に基づいて、所望のファイルが格納されたセクタアドレスを管理している。

【0221】国際標準化機構によりISO13346において規定されたファイルシステムの構造では、書き換え可能型光ディスクに対応するために、ファイルの記録位置はファイルエントリと呼ばれる情報を用いて管理される。図32に示すように、例えば、ファイル(1)2703の記録位置のデータは、ファイル管理情報領域2751内のファイルエントリ(1)2701として格納され、ファイル(2)2704の記録位置のデータはファイルエントリ(2)2702として格納される。各ファイルは、光ディスク上で連続した複数のセクタの領域を管理するエクステント2706、2708で構成される。光ディスク上には、ファイルエントリが示すメインデータ領域2102において、第7の実施形態で示した暗号化コンテンツが記録され、また、復号鍵がリードイン領域2601内の復号鍵テーブル2707に記録される。暗号化コンテンツが記録されたユーザデータ領域2602内のセクタヘッダ領域2101には、復号に必要な復号鍵を参照するための記録位置を示すポインタが、鍵インデックス領域2708において記録される。なお、本実施形態では、ファイル単位とエクステント単位で復号鍵を管理して記録しているが、本発明はこれに限らず、ファイル単位とエクステント単位とのうちの少なくとも一方で復号鍵を管理して記録してもよい。

【0222】上記のようにファイルシステムにより管理される光ディスクにおいて、著作権保護を必要とするコンテンツの記録動作について図33を用いて説明する。図33は、第8の実施形態に係るファイル管理システムによって実行される、著作権保護を必要とするコンテンツの記録処理を示す。

【0223】暗号化コンテンツの記録の際には、まず、ステップS2801において、図30(b)に図示された復号鍵状態テーブル2502を読み出して、復号鍵テーブル2707の空き領域を調べる。次いで、ステップS2802において、復号鍵テーブル2707の空き領域があるか否かが判断され、NOのときは、暗号化コンテンツに対する復号鍵が記録できないために、ステップS2807において記録動作を中止して当該コンテンツの記録処理を終了する。一方、ステップS2802でYESであるときは、取得済みの復号鍵（又はタイトル鍵）を記録し、また、復号鍵を取得できていない場合には、復号鍵領域の予約を行う。次いで、ステップS2804では、記録するコンテンツの著作権制御情報（暗号化を行うか否かの情報と、暗号化の種類を示す種別の情報などを含む。）と、鍵インデックス領域2708に記録する鍵インデックスの設定を行った後、ステップS2806においてコンテンツを暗号化してエクステント単位でファイル形式で光ディスク上に記録する。このと

き、ファイル単位で同一の著作権制御情報と鍵インデックスを使用してもよいし、エクステント単位でこれらを切り替えてもよい。すなわち、ステップS2804及びS2805において、処理する単位は、ファイル単位と、エクステント単位とのうちの少なくとも一方である。最後に、ステップS2806において、記録したコンテンツに関する情報に基づいて、上記記録されたデータを管理するためのファイル管理情報の更新を行った後、当該コンテンツの記録処理を終了する。

【0224】図34は、第8の実施形態に係るファイル管理システムによって実行される、コンテンツの再生処理を示すフローチャートである。図34では、図33に示した方法によりファイル形式で記録したコンテンツを光ディスクから再生する処理を示す。

【0225】ファイルの再生動作を行う際には、再生するファイルが使用している復号鍵テーブルの領域を知るため、ファイル管理情報領域2761内のファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ステップS2901において、ファイル管理情報2761から再生するファイルのファイルエントリを読み出して再生することにより取得した後、ステップS2902において、ファイルエントリにより示される領域のセクタヘッダ領域2102から鍵インデックス領域の値を読み出して再生することにより取得する。エクステント単位で異なる暗号を行っている場合には、それぞれのエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次いで、ステップS2903において、取得した鍵インデックスにより示される復号鍵テーブル2707の復号鍵領域から復号鍵を読み出して再生することにより取得する。さらに、ステップS2904において、ファイルエントリで示される領域からファイル内のコンテンツのデータを読み出して再生し、再生したコンテンツのデータを復号する。ここで、コンテンツのファイルの再生と復号が終了すれば、当該コンテンツの再生処理を終了する。

【0226】図35は、第8の実施形態に係るファイル管理システムによって実行される、コンテンツの削除処理を示すフローチャートであり、図35では、図33に示した方法により記録したファイル形式のコンテンツのデータを削除する動作について示す。

【0227】ファイルの削除動作を行う際には、削除するファイルが使用している復号鍵テーブル2707の領域を知るため、ファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ステップS3001において、ファイル管理情報領域2761内のファイル管理情報から削除するファイルのファイルエントリを取得した後、ステップS3002においてファイルエントリにより示される領域のセクタヘッダから鍵インデックス領域の値を取得する。ここで、エクステント単位で異なる暗号を行っている場合には、それぞれ

のエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次いで、ステップS3003において、取得した鍵インデックスにより示される復号鍵テーブル2707の復号鍵領域から復号鍵を開放した（ここで、復号鍵の開放とは、当該復号鍵を当該テーブルから削除することをいう。）後、ステップS3004において削除するファイルの書き込み位置を示すファイルエントリをファイル管理情報から削除して、当該コンテンツの削除処理を終了する。従来のファイルシステムでは、ファイルを削除する際にファイルエントリのみの削除を行っていたが、復号鍵と暗号化コンテンツの記録セクタが別の領域に記録されているために、別の領域に記録された復号鍵を削除できない。上述の実施形態においては、ファイルエントリの削除に先立って、セクタヘッダ領域中の鍵インデックスの示す復号鍵を復号鍵テーブル2707から削除することにより、光ディスク上での復号鍵の管理を行っている。

【0228】<第9の実施形態>図36は、本発明に係る第9の実施形態である光ディスクシステムの構成を示すブロック図であり、この光ディスクシステムは、光ディスク3100に著作権保護を必要とするコンテンツを記録及び再生する情報処理システムである。当該光ディスクシステムは、エンコード装置3101と、光ディスク装置3102と、デコード装置3103と、パーソナルコンピュータ3104とを備えて構成される。

【0229】エンコード装置3101は、コンテンツのデータを格納するコンテンツメモリ3131と、上記コンテンツのデータをMPEGフォーマットの形式で符号化する符号化回路3132と、暗号鍵を格納する暗号鍵メモリ3133と、符号化されたコンテンツのデータを暗号鍵を用いて暗号化するとともに復号鍵を生成して復号鍵メモリ3111に格納する暗号回路3134と、復号鍵を格納する復号鍵メモリ3111と、復号鍵をバス暗号化するバス暗号回路3112と、パーソナルコンピュータ3104のインターフェース3122にPCIバス3151を介して接続され暗号化されたコンテンツのデータや復号鍵を送信するインターフェース3124とを備える。また、光ディスク装置3102は、複数の復号鍵を格納する復号鍵テーブルメモリ3113と、バス暗号及び復号回路3114と、光ディスク3100に対してデータを記録するとともに光ディスク3100からデータを読み出して再生する記録再生回路3119と、パーソナルコンピュータ3104のインターフェース3121とSCSIバス3152を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース3120とを備える。なお、SCSIバス3152はATAPIバスであってもよい。ここで、バス暗号化及びバス復号化とはそれぞれ、PCIバス3151やSCSIバス3152上で暗号鍵や復号鍵を暗号化して送信し受信するために

用いる暗号化処理、及び復号化処理をいう。

【0230】さらに、パーソナルコンピュータ3104は、その動作を制御する制御部3130と、複数のバス暗号化復号鍵を格納するバス暗号化復号鍵テーブルメモリ3115と、上記複数のバス暗号化復号鍵に対応する複数の復号鍵ステータス（復号鍵の記録状態を示し、具体的には、未使用、領域予約、鍵記録済み、予約済みなどを示す。）のデータを格納する復号鍵状態テーブルメモリ3116と、光ディスク装置3102のインターフェース3120とSCSIバス3152を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース3121と、デコード装置3103のインターフェース3123及びエンコード装置3101のインターフェース3124とPCIバス3151を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース3122とを備える。またさらに、デコード装置3103は、パーソナルコンピュータ3104のインターフェース3122と接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース3123と、インターフェース3123によって受信された暗号化復号鍵をバス復号化するバス復号回路3117と、復号鍵を格納する復号鍵メモリ3118と、インターフェース3123によって受信された暗号化コンテンツのデータを復号鍵メモリ3118の復号鍵を用いて復号するとともに、MPEGフォーマットの復号化処理を行って画像信号や音声信号を生成してディスプレイ装置3105に出力する復号化回路3141とを備える。

【0231】この光ディスクシステムのエンコード装置3101においては、符号化回路3132は、コンテンツメモリ3131に格納され又は入力されるAVデータなどのコンテンツのデータをMPEGのフォーマットの形式で符号化し、暗号回路3134は、パーソナルコンピュータ3104上でのコンテンツの不正利用を避けるために生成された暗号鍵メモリ3133内の暗号鍵を用いて上記符号化されたコンテンツのデータを暗号化し、暗号化されたコンテンツのデータをインターフェース3124及びパーソナルコンピュータ3104を介して光ディスク装置3102に送信する。ここで、暗号化されたコンテンツのデータは、エンコード装置3101のインターフェース3124からPCIバス3151と、パーソナルコンピュータ3104のインターフェース3122及びインターフェース3121と、光ディスク装置3102のインターフェース3120を介して記録再生回路3119に送信される。そして、暗号化されたコンテンツのデータは、光ディスク装置3102の記録再生回路3119により光ディスク3100に記録される。また、光ディスク装置3102の記録再生回路3119は、光ディスク3100に記録されている暗号化コンテ

ンツのデータを再生して、再生された暗号化コンテンツのデータを、インターフェース3120と、パーソナルコンピュータ3104のインターフェース3121及びインターフェース3122と、デコード装置3103のインターフェース3123を介して復号化回路3141に送信する。デコード装置3103の復号化回路3141は、暗号化コンテンツのデータに対する暗号を復号化しかつMPEGフォーマットの復号化処理を行い、復号化されたコンテンツの画像信号や音声信号をそれぞれディスプレイ装置3105やスピーカ装置（図示せず。）に出力する。

【0232】エンコード装置3101の暗号回路3134は、MPEGフォーマットの形式で符号化されたコンテンツのデータに対して、暗号鍵メモリ3133内の暗号鍵を用いて暗号化を行うと同時に、再生時に必要な復号鍵を生成して復号鍵メモリ3111に格納する。光ディスク3100には、符号化されたコンテンツのデータと復号鍵を記録する必要があるが、パーソナルコンピュータ3104上で復号鍵を平文のまま取り扱う場合には、復号鍵を光ディスク3100から読み出すことにより、暗号化されたコンテンツのデータの解読が容易になってしまう可能性がある。これを避けるために、エンコード装置3101と光ディスク装置3102の間で、相互認証を行うとともに相互に共有したバス鍵を用いてバス暗号を行う。

【0233】すなわち、具体的には、復号鍵メモリ3111内の復号鍵はエンコード装置3101のバス暗号回路3112によって暗号化が施された後、その暗号化復号鍵は、インターフェース3124、PCIバス3151及びインターフェース3122を介してパーソナルコンピュータ3104のバス暗号化復号鍵テーブルメモリ3115に格納される。一方、光ディスク装置3102のバス暗号及び復号回路3114においては、光ディスク3100から記録再生回路3119により再生された、暗号化復号鍵の復号化が行われた後、復号化された復号鍵は復号鍵テーブルメモリ3113に格納される。また、バス暗号及び復号回路3114は、例えば更新されたバス暗号化された復号鍵を、バス暗号化復号鍵テーブルメモリ3116からインターフェース3121、SCSIバス3152及びインターフェース3120を介して受信してバス復号化して復号鍵テーブルメモリ3113に格納した後、記録再生回路3119を介して光ディスク3100に記録する。

【0234】また、復号鍵状態テーブルは記録再生回路3119により光ディスク3100から再生された後、インターフェース3120、SCSIバス3152及びインターフェース3121を介して復号鍵状態テーブルメモリ3116に転送されて格納される。さらに、パーソナルコンピュータ3104で更新された復号鍵状態テーブルは、復号鍵状態テーブルメモリ3116から読み